PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA SECRETARÍA DE EDUCACIÓN DEL MUNICIPIO DE YUMBO, EN CUMPLIMIENTO DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA DE COLOMBIA

HAMES VARGAS POLANCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍA

MAESTRÍA EN GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN

SANTIAGO DE CALI

2019

PLAN DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA SECRETARÍA DE EDUCACIÓN DEL MUNICIPIO DE YUMBO, EN CUMPLIMIENTO DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA DE COLOMBIA

HAMES VARGAS POLANCO

Trabajo de grado para optar al título de Magister en Gestión de Tecnologías de Información

Director

ANIVAR NESTOR CHAVES TORRES

Ph(C) en Ciencias de la Educación

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍA

MAESTRÍA EN GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN

SANTIAGO DE CALI

2019

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Jurado

_____

Jurado

Santiago de Cali, Mayo de 2019

Dedico este triunfo a mi Madre Alba Esneda Polanco, por darme la vida, comprenderme, esforzarse y apoyarme para tener una buena formación personal y académica, a mi padre Alipio Vargas Salazar (QEPD), por su apoyo incondicional, a mi esposa Darly Adriana Hernández Peña por su inmenso amor, acompañamiento y comprensión, a mis hijas Leidy Viviana, Diana Alexandra y Carolina, por ser mi razón de vivir, a mis nietos Juan Camilo, Laura Sofía y Thomas, por la alegría y gran motivación que me han dado con su presencia.

Agradecimientos

Le doy infinitas gracias a Dios por permitirme alcanzar un logro más en mi vida.

A Rodrigo Sánchez Gaviria por su apoyo incondicional y motivación para ser cada vez mejor.

A mis hermanos Maricel, Rodrigo y Rubén Darío por ser mis modelos de superación y perseverancia.

A mi Director, Anivar Nestor Chaves Torres, por ser mi guía, orientador y por el apoyo dado para la culminación del presente proyecto.

Al Doctor Jorge Enrique Portella Cleve y grupo de docentes de la UNAD por su paciencia, orientación, acompañamiento y gestión en mi proceso de aprendizaje.

Al Secretario de Educación y al líder TIC del Municipio de Yumbo, por permitirme realizar el presente proyecto en la Alcaldía de Yumbo.

Contenido

Pág.

Resumen 19

Abstract 20

Introducción 21

Contextualización 21

Capítulo 1: Aspectos generales de la Investigación 23

1.1. El problema 23

1.2. Objetivos 26

1.2.1. Objetivo general 26

1.2.2. Objetivos Específicos 26

Capítulo II. Fundamentación Teórica 27

2.1. Estado del Arte de Seguridad y Privacidad de la Información 27

2.2. Marco teórico-conceptual 29

2.2.1. Seguridad de la información 29

2.2.2. Vulnerabilidades y amenazas 30

2.2.3. Análisis y gestión de riesgo 31

2.2.4. Metodologías de análisis y gestión de riesgo 32

2.2.5. Sistema de Gestión de Seguridad de la información 40

2.2.6. Modelo de Seguridad y Privacidad de la Información (MSPI) 41

Capítulo III. Metodología. 45

3.1. Etapas previas a la implementación. 46

3.2. Etapa de Planificación 47

3.3. Población y muestra 48

Capítulo IV. Estado actual de la gestión de seguridad de la información en la Secretaría de Educación del Municipio de Yumbo. 55

4.1. Políticas de seguridad de la información (control a.5) 57

4.2. Organización de la seguridad de la información (Control A.6) 58

4.3. Seguridad de los recursos humanos (Control A.7) 60

4.4. Gestión de activos (Control Número A.8) 61

4.5. Control de acceso (Control A.9) 62

4.6. Criptografía (Control A.10) 62

4.7. Seguridad física y del entorno (Control A.11) 63

4.8. Seguridad de las operaciones (Control A.12) 64

4.9. Seguridad de las comunicaciones (Control A.13) 65

4.10. Adquisición, desarrollo y mantenimiento de sistemas (Control A.14) 66

4.11. Relaciones con los proveedores (Control A.15) 68

4.12. Gestión de incidentes de seguridad de la información (Control A.16) 69

4.13. Aspectos de seguridad de la información de la gestión de la continuidad del negocio (Control A.17) 70

4.14. Cumplimiento (Control A.18) 71

Capítulo V. Plan de seguridad y privacidad de la información 74

5.1. Inventario de activos de información 74

5.1.1 Inventario de recursos tecnológicos y humanos 74

5.2 Identificación, valoración y tratamiento de riesgo 74

5.2.1 Contexto estratégico..... 75
5.2.2 Criterios básicos..... 90
5.2.3 Identificación y Análisis del riesgo..... 92
5.2.4 Identificación de vulnerabilidades de los activos de información ante amenazas potenciales 147
5.3. Política de seguridad y privacidad de la información..... 163
5.3.1. Política general de seguridad y privacidad de la información del municipio de Yumbo . 163
5.3.2. Alcance/Aplicabilidad 165
5.4. Manual de política de seguridad y privacidad de la información 169
5.4.1. Objetivos y Alcance..... 169
5.4.2. Marco de referencia 170
5.4.3. Misiones generales y particulares 172
5.4.4. Acciones que afectan la seguridad de la información..... 176
5.4.5. Procedimientos de seguridad y privacidad de la información 178
5.4.6 Sanciones previstas por incumplimiento 209
5.5. Roles y responsabilidades de seguridad y privacidad de la información..... 210
5.5.1. Definición de roles y responsabilidades 210
Capítulo VI. Plan de comunicación, sensibilización y capacitación sobre la importancia de la seguridad y privacidad de la información..... 220
6.1. Presentación 220
6.2 Justificación 220
6.3. Objetivos..... 221
6.3.1. Objetivo general..... 221
6.3.2. Objetivos específicos 222
6.4 Actividades 222
6.4.1. Diseño del programa de comunicación, sensibilización y capacitación. 222
6.4.2. Identificación de necesidades 223

6.4.3. Diseño del plan de capacitación y sensibilización 224
Conclusiones 229
Referencias Bibliográficas 235
Anexos 242

Lista de tablas

Tabla 1. Metas, resultados e Instrumentos en el Diagnóstico 42
Tabla 2. Metas, Resultados e Instrumentos Fase de planificación 43
Tabla 3. Responsables y áreas involucradas 50
Tabla 4. Escala de Valoración de Controles ISO 27001 56
Tabla 5. Funciones secretario de educación Yumbo 79
Tabla 6. Funciones del subsecretario de Calidad y cobertura 82
Tabla 7. Funciones Líder TIC Secretaría de Educación 85
Tabla 8. Personal TIC Secretaría de educación Yumbo 89
Tabla 9. Grupo de activos 93
Tabla 10. Activos de Información 97
Tabla 11. Valoración de los Activos 101
Tabla 12. Matriz para la valoración de amenazas - ámbito: instalaciones 106
Tabla 13. Matriz para la valoración de Amenazas - ámbito: hardware 107
Tabla 14. Matriz para la valoración de amenazas - ámbito: aplicaciones 109
Tabla 15. Matriz para la valoración de amenazas - ámbito: datos 111
Tabla 16. Matriz para la valoración de amenazas - ámbito: red de comunicaciones 113
Tabla 17. Matriz para la valoración de amenazas - ámbito: servicios 115
Tabla 18. Matriz para la valoración de amenazas - ámbito: equipamiento auxiliar 117
Tabla 19. Matriz para la valoración de amenazas ámbito: personal o recurso humano 119
Tabla 20. Impacto potencial 122
Tabla 21. Modelo de capacidad CMM 129
Tabla 22. Nivel de riesgo aceptable y riesgo residual 133
Tabla 23. Proyectos de Seguridad propuestos 145
Tabla 24. Responsabilidades - marco de arquitectura empresarial 213

Lista de figuras

Figura 1. Proceso para la administración del Riesgo en Seguridad de la Información 32
Figura 2. ISO31000 - Marco de trabajo para Gestionar Riesgos 34
Figura 3. Componentes Modelo MAGERIT 36
Figura 4. Marco de seguridad y privacidad de la información 46
Figura 5. Etapas previas a la implementación 46
Figura 6. Fase de Planificación 47
Figura 7. Datos Básicos Portada 55
Figura 8. Evaluación de Efectividad de Controles - ISO 27001:2013 Anexo 1 72
Figura 9. Brecha Anexo 1 ISO 27001:2013 73
Figura 10. Organigrama Municipio de Yumbo 76
Figura 11. Organigrama Secretaría de Educación Yumbo 78
Figura 12. Organigrama grupo TIC SEM Yumbo 90
Figura13. Rangos de Valoración del Riesgo 100
Figura 14. Importancia de los activos 100
Figura 15. Formato para Valoración de amenazas 105
Figura 16. Puerta de acceso al Datacenter 147
Figura 17. Racks de comunicaciones 149
Figura 18. Racks de servidores 150
Figura 19. Racks de Monitoreo de cámaras de seguridad 151
Figura 20. Consola de Monitoreo de servidores 152
Figura 21. Organización Datacenter 1 153
Figura 22. Puerta de acceso al Datacenter 153
Figura 23. Organización del Datacenter 2 155
Figura 24. Organización de los Rack de comunicaciones 156
Figura 25. Aplicación de gestión de activos 157
Figura 26. Control de acceso a la red de la Alcaldía de Yumbo 157
Figura 27. Seguridad privada y cámaras de video vigilancia 158
Figura 28. Seguridad de las Comunicaciones 159
Figura 29. Seguridad UPS 160
Figura 30. Pruebas al portal www.yumbo.gov.co 162

Lista de Anexos

Anexo 1. Carta de aceptación anteproyecto MinTIC..... 242

Anexo 2. Carta de presentación y aceptación Municipio de Yumbo..... 243

Anexo 3. Certificación nuevo Líder TIC Yumbo 244

Resumen

Actualmente la información es tomada como un activo supremamente importante para la organización, lo que conlleva a una responsabilidad de salvaguardarla y gestionarla adecuadamente pues cada vez son más intensos y sofisticados los ataques de delincuentes informáticos a los sistemas de información, quienes cada vez están buscando vulnerabilidades de los sistemas de información para acceder a ellos y acatarlos.

Por lo anterior, las organizaciones cuentan con herramientas y marcos de referencia - como la norma ISO-27001 que busca preservar la confidencialidad, integridad y disponibilidad de la información - asociados a los sistemas que hacen parte de su tratamiento en la organización. Por otra parte, garantizar la seguridad total de la información es casi imposible, por lo que las organizaciones deben estar atentas a cualquier situación que pueda comprometerla, implementando y manteniendo controles para mitigar los riesgos.

En este proyecto se realiza un análisis del estado actual de la Seguridad de la Información en la Secretaría de Educación del Municipio de Yumbo, el cual permite elaborar el Plan de Gestión de Seguridad de la Información y, asociado al mismo, el Plan de Comunicación, Sensibilización y Capacitación sobre la importancia de la seguridad y privacidad de la información, lo anterior basado en el Modelo de Seguridad y Privacidad de la Información MSPI de la estrategia de gobierno en Línea propuesta por el Ministerio de Tecnologías de Información y Comunicaciones de Colombia.

Palabras Claves: Sistemas, información, informática**,** organización, Norma ISO, comunica

Abstract

Currently, information is taken as a supremely important asset for the organization, which entails a responsibility to safeguard and manage it appropriately, as attacks by computer criminals on information systems are becoming more intense and sophisticated, computer criminals are increasingly looking for vulnerabilities in the information systems to access them and comply with them.

Therefore, organizations have tools and frameworks such as ISO-27001, which seeks to preserve the confidentiality, integrity and availability of information, associated with the systems that are part of their treatment in the organization. From elsewhere, guaranteeing the total security of information is almost impossible, so organizations must be alert to any situation that may compromise it, implementing and maintaining controls to mitigate risks.

This project is an analysis of the current state of Information Security in the Ministry of Education of the Municipality of Yumbo, which allows the development of the Information Security Management Plan and associated with it, the Communication Plan, Awareness and

Training on the importance of information security and privacy, the foregoing based on the MSPI Information Security and Privacy Model of the online government strategy proposed by the Ministry of Information and Communication Technologies of Colombia.

Keywords: Systems, information, computing, organization, ISO Standard, communication

Introducción

Contextualización

Actualmente, las personas y las organizaciones son conscientes de la importancia de la seguridad de la información, pues son muchos los casos de ataques cibernéticos realizados a sistemas de información por delincuentes informáticos; por lo anterior, se le reconoce como un concepto sistémico global que debe hacer parte importante de los procesos de negocio, reconocido por los ejecutivos de la empresa y toda la comunidad de la organización aplicable a los activos de información de la entidad.

La Secretaría de Educación Municipal de Yumbo, Valle del Cauca, como ente certificado en educación, es la entidad encargada de gestionar la información de toda la comunidad educativa del Municipio y como tal, de acuerdo con las directivas establecidas por el Ministerio de Tecnologías e Información de Colombia, tiene que cumplir con la estrategia de Gobierno en Línea, entre otros, con el componente de seguridad y privacidad de la información, el cual es el eje que se aborda en el presente Proyecto, buscando garantizar los principios de confidencialidad, integridad, disponibilidad y autenticidad de la información.

En el presente informe de investigación, se muestran datos estructurados y evidencias necesarias para la elaboración del Proyecto, cuyo objetivo fue diseñar un Plan de Gestión de la Seguridad de la Información para la Secretaría de Educación del Municipio de Yumbo, en cumplimiento de la estrategia de gobierno en línea de Colombia, que se derivó de un diagnóstico previo. El Plan es el insumo más importante para la implementación del Sistema, el cual permitirá minimizar los riegos de ataques por parte de delincuentes informáticos, y, que a su vez este sirva para la elaboración y/o actualización del Modelo de Seguridad y Privacidad de la Información (MSPI) del Municipio de Yumbo.

La Investigación se desarrolló bajo el paradigma cuantitativo, con un estudio de tipo descriptivo y para el diseño se aplicó el modelo de seguridad de la información de Gobierno en línea de Colombia, hoy denominado Política de Gobierno Digital.

El documento está organizado por capítulos, en el primero se aborda el problema de investigación donde se describe la naturaleza y magnitud del problema que se espera resolver con el desarrollo del Proyecto y se detalla la fundamentación teórica en donde se revisan el conjunto de conocimientos, técnicas y metodologías existentes para desarrollar el mismo, En el segundo se realiza el diagnóstico para determinar el nivel actual en materia de seguridad y privacidad de la información y en el tercer capítulo se propone el Plan de seguridad y privacidad de la información.

Desde el punto de vista normativo se destaca el Decreto 1413 (MinTIC, 2017), "Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales", Con lo anterior cada vez Colombia se ajusta a los cambios y exigencias que en materia de seguridad y privacidad de la información se plantean a nivel internacional.

Capítulo 1: Aspectos generales de la Investigación

1.1. El problema

La información es uno de los activos más preciados para las organizaciones, pero también es el más sensible y el que más riesgos enfrenta, especialmente al gestionarse a través de redes telemáticas. Teniendo en cuenta lo manifestado por (Organización de estados Americanos OEA y AWS, 2018) quien refiere que:

> Cada día se producen más de 230.000 muestras diferentes de malware y la tendencia es que este número vaya creciendo. También a diario se denuncian más de 4.000 ataques de *ransomware*. Este crecimiento continuo en las cifras de ataques está motivado por el beneficio económico potencial que el ciber criminal espera obtener, habiendo estimaciones que apuntan a que las perdidas asociadas con los delitos informáticos alcance la cifra de 2,1 billones de dólares en 2019 (p.9).

Lo anterior ratifica la necesidad que todos los países diseñen he implementen estrategias para proteger la información de sus ciudadanos, bajo este contexto a continuación se relacionan marcos legales aplicados en algunos países:

En España, existe la ley Orgánica 15/1999 de protección de datos de carácter personal (Portal de la Transparencia España, 2016), que pretende garantizar y proteger, en lo que concierne al tratamiento de los datos personales y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar

En el mismo sentido, en chile existe la Ley 19.628 del 28 de agosto de 1999 (Secretaria General de la Presidencia Chile, 1999), que aborda la misma problemática teniendo como como marco jurídico la presente norma.

Por su parte Colombia cuenta con la Ley Estatutaria 1581 del año 2012 (Congreso de la república de Colombia, 2018), reglamentada parcialmente por el Decreto 1377 de 2013 (Ministerio de Comercio, Industria y Turismo de Colombia, 2013, P.1), "Por la cual se dictan disposiciones generales para la protección de datos personales".

La normatividad referenciada parte de las restricciones de acceso a los datos que deben ser protegidas por las entidades que tengan a cargo la disposición de este, es por ello que se contextualiza sobre la definición de Dato a continuación.

Se define el dato personal como: "cualquier información concerniente a una persona", esta información de los ciudadanos se almacena en repositorios de datos (bases de datos de entidades públicas y privadas), para el desarrollo de sus actividades (Perez, 2016).

La sensibilidad de los datos se establece en función del daño que se le puede causar a una persona al revelar o divulgar dicha información sin su autorización.

Teniendo en cuenta lo anterior, la Ley Orgánica de Protección de Datos de carácter Personal (LOPD), establece una serie de requisitos tanto para la adquisición como para la conservación y cesión de los datos, siendo más exigente cuando mayor es la sensibilidad de la información recogida.

El título II en su Artículo 4°de la mencionada Ley, trata sobre los Principios para el Tratamiento de datos personales, los cuales son: Principio de legalidad en materia de tratamiento de datos, Principio de veracidad o calidad, Principio de finalidad, Principio de transparencia, Principio de libertad, Principio de acceso y circulación restringida, Principio de seguridad y Principio de confidencialidad.

Siendo coherente con lo anterior, seguidamente se describe cómo el Municipio de Yumbo dadas sus características, debe aplicar lo establecido por la estrategia de gobierno en línea y dar

cumplimiento a la normatividad en materia de protección de datos personales referida con anterioridad, por lo que describe su caracterización y problemática:

El Municipio de Yumbo hace parte de los 42 Municipios del Departamento del Valle del cauca, Tiene Categoría Uno, 114.000 habitantes, más de 2.800 Empresas (por eso se le denomina como capital Industrial del Valle del Cauca), con un presupuesto de ingresos para la vigencia 2018 que asciende a $282.758.626.981 (Municipio de Yumbo, 2017).

En el plan de desarrollo de Yumbo 2016-2019 (Municipio de Yumbo, 2016) denominado "Yumbo territorio de oportunidades para la gente", en el numeral 3.3 de fortalecimiento institucional, en el programa tecnologías de la información y la comunicación, se proyecta la ejecución del meta producto "Implementar el plan estratégico de las tecnologías de la información y las comunicaciones, PETIC".

El PETIC, establece algunos procedimientos para el aseguramiento de la disponibilidad de la información contenida en las bases de datos entre otros, pero no detalla las recomendaciones que a nivel general debe cumplir el Municipio en el marco de la estrategia de Gobierno en línea en materia de seguridad de la información.

Hay que tener en cuenta que el Municipio de Yumbo por ser una entidad perteneciente al Sector Gobierno del estado Colombiano, debe cumplir con lo estipulado en la ley 1273 de 2009 (Congreso de Colombia, 2009) y con la Estrategia de Gobierno en Línea Decreto 2573 de 2014 (Ministerio de Tecnologías de Información y Comunicaciones, 2014), título II componentes, instrumentos y responsables, Artículo 5 Componentes, literal 4 Seguridad de la información, que establece "Comprende las acciones transversales a los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada".

El presente proyecto de investigación pretende dar respuesta a la siguiente pregunta: ¿Cómo mejorar la seguridad de la información y dar cumplimiento a la estrategia de gobierno en línea de Colombia en la Secretaría de Educación del Municipio de Yumbo?

1.2. Objetivos

1.2.1. Objetivo general

Diseñar un Plan de Gestión de la Seguridad de la Información para la Secretaría de Educación del Municipio de Yumbo, en cumplimiento de la estrategia de gobierno en línea de Colombia.

1.2.2. Objetivos Específicos

- Determinar el estado actual de la gestión de seguridad de la información en la Secretaría de Educación del Municipio de Yumbo.
- Elaborar el Plan de Seguridad y Privacidad de la Información para el SGSI.
- Diseñar un plan de comunicación, sensibilización y capacitación sobre la importancia de la Seguridad y Privacidad de la Información para la Secretaría de Educación de Yumbo.

Capítulo II. Fundamentación Teórica

2.1. Estado del Arte de Seguridad y Privacidad de la Información

Los grandes avances que muchos países al rededor del mundo han presentado en materia de e-Gobierno han permitido impulsar el desarrollo económico, social y cultural como también el político, beneficiando a diversos sectores, comunidades y ciudadanos. Un análisis detallado de la situación específica que al momento presentan los diferentes países se puede consultar en el reporte publicado en (ONU, 2016) sobre e-Gobierno que desde 2003 adelantan las Naciones Unidas. En el reporte del 2016 se destaca que hay un fuerte aumento en el número de países que utilizan el gobierno electrónico para proporcionar servicios públicos en línea a través de plataformas integrales, 90 países ofrecen servicios en línea y 148 países ofrecen al menos una forma de servicio transaccional en línea, lo anterior lleva a la reflexión sobre la importancia de implementar medidas de protección a la información de los ciudadanos.

Al respecto la Organización de las Naciones Unidas (ONU, 2018) manifiesta que la lucha contra el ciberterrorismo y la ciberdelincuencia debe comprender una doble vertiente, el ciberespacio como herramienta que permite el desarrollo de actividades delictivas y como objetivo final de la acción, por lo que se requiere la colaboración de distintos actores y que sea abordada de forma integral, teniendo en cuenta temas como conocimiento y experiencia sobre amenazas y vulnerabilidades relacionadas con la delincuencia cibernética.

Según el ESET *Security Report* Latinoamérica 2017 (ESET, 2017), el cual resume incidentes de seguridad en 13 países y más de 4000 personas encuestadas en Latinoamérica, se destaca que un 49% de las respuestas fueron afirmativas en haber sido atacadas por código malicioso o malware, es decir una de cada dos empresas latinoamericanas fueron atacadas. A nivel de ataques continúa *rasomware* con 16%, *phishing* con 15%, explotación de

vulnerabilidades 10%, ataques de denegación de servicios 9%, acceso indebido de aplicaciones y bases de datos 9%, falta de disponibilidad de servicios críticos 8% y por último los fraudes internos con 7%, por lo que se requiere de implementar acciones que permitan minimizar estos riesgos. Dentro de las infecciones malware por país Colombia ocupa un tercer lugar con 46.7%, por debajo de Panamá con 50.3% y Nicaragua con 53%.

Por otra parte (SYMANTEC, 2018), destaca como el *cryptojacking* ha tenido un crecimiento de 8500%, los ataques a la cadena de suministro y el malware en los dispositivos móviles encabezan la innovación en el panorama de las amenazas, así mismo detalla que gran parte de los delincuentes que dirigen ataques especializados emplean métodos tradicionales con efectos devastadores o catastróficos para las organizaciones y en el 2017 el 71% de los ataques empezaron por *spear phishing*. Se resalta como los atacantes están cada vez más capacitados, disponen de recursos y pueden apropiarse de información valiosa o causar interrupciones graves a los sistemas de información.

Según lo establece el Procedimiento de seguridad de la información en Colombia (MinTIC, 2016), para el desarrollo del componente de Seguridad y Privacidad de la Información, el Ministerio de TIC de Colombia ha diseñado un documento de lineamientos denominado "Modelo de Seguridad y Privacidad de la Información", documento que se ha actualizado en los últimos años, teniendo en cuenta las actualizaciones de la norma técnica que le sirve de sustento como lo es la ISO 27001, las mejores prácticas en seguridad de TI y los cambios normativos que tengan impacto sobre el mismo. En este mismo sentido se encuentra que el MSPI, se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia como lo son: TIC para Servicios, TIC para Gestión y TIC para Gobierno Abierto.

2.2. Marco teórico-conceptual

El desarrollo del informe del proyecto se enmarca en el concepto seguridad de la información, por lo cual resulta muy adecuado iniciar por precisar el significado de este concepto, para posteriormente definir lo concerniente a las vulnerabilidades y amenazas a los sistemas de información, como también la gestión del riesgo y las metodologías para el análisis.

2.2.1. Seguridad de la información

Toda entidad debe tener una estrategia de seguridad y privacidad de la información, que le permita llegar a un estado de madurez o capacidad deseado en esta misma materia. Dentro de la estrategia debe contemplar tres pilares fundamentales para la correcta gestión de la información, que según (MinTIC, 2015) son:

- Confidencialidad: En este aspecto la información solo debe ser accedida por los destinatarios autorizados.
- Integridad: Se busca que la información debe ser a exacta, fiable y completa.
- Disponibilidad: La información debe estar accesible y disponible cuando se le requiera.

Lo anterior implica que el proceso de seguridad de la información busque el cumplimiento de metas y objetivos de la organización, la información sea confiable y utilizada solo por las personas autorizadas para hacerlo.

Según lo referencia (ISACA, 2018), la Seguridad de la Información es por lo general la principal prioridad para el Gerente de Sistemas de Información (CIO), quien debe garantizar un enfoque de mayor a menor criticidad y la cultura de trabajo orientada a la Seguridad de la Información al interior de la organización. Una vía práctica de iniciación para el Gerente de Sistemas en temas de seguridad de información es trabajar conjuntamente con el Oficial de Seguridad (CISO) para definir un marco de gobierno de manera que este asuma la responsabilidad operativa en su totalidad.

La gestión de la seguridad de TI se trata de tomar decisiones para mitigar el riesgo, mientras que el gobierno determina quién está autorizado para tomar decisiones. El gobierno de seguridad de la información se refiere a la dirección, la estructura organizativa, roles y responsabilidades, y diversos procesos establecidos para la seguridad de la información. Mientras la gestión recomienda estrategias de seguridad, gobierno asegura que las estrategias de seguridad estén alineadas con los objetivos de negocio y de conformidad con la regulación vigente

2.2.2. Vulnerabilidades y amenazas

Se define vulnerabilidad como una fragilidad o debilidad del sistema informático que puede utilizar un delincuente informático para causar un daño. (MinTIC, 2016), manifiesta que pueden existir vulnerabilidades a nivel de hardware, software, red, personal, lugar y organización, los cuales pueden generar diferentes tipos de amenazas con graves consecuencias para la entidad.

La Guía de gestión de riesgos (MinTIC, 2016), establece que una amenaza tiene gran probabilidad de causar daños a activos de la organización como la información, los sistemas y procesos, por lo tanto, a la entidad. Las amenazas pueden ser de origen humano o natural y podrían ser deliberadas o accidentales, por lo que es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Eventos Naturales, Daño Físico y por ende pérdidas de los servicios esenciales, Perturbación debido a emisión de radiaciones, acciones sin autorización, fallas técnicas o amenazas humanas, entre otras).

Según lo define el Gobierno de España, (2012) , una vulnerabilidad es toda debilidad que puede ser aprovechada por una amenaza o delincuente, a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial. (p.8), es decir, se consideran vulnerabilidades todas las ausencias o falencias en las salvaguardas pertinentes para

proteger el valor propio o acumulado sobre un activo. Algunas veces se usa el término "insuficiencia" para destacar el hecho de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza.

2.2.3. Análisis y gestión de riesgo

El Departamento Administrativo de la Función Pública –DAFP- (2011) hace una diferenciación entre gestión del riesgo y gestionar el riesgo, en donde se aclara que la gestión del riesgo se refiere a los principios y metodología para la gestión eficaz del riesgo y por otra parte gestionar el riesgo se refiere a la **"aplicación de estos principios y metodología a riesgos particulares";** se entiende entonces que la administración del riesgo "comprende el conjunto de Elementos de Control y sus interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales". Lo anterior permite que la organización consolide su Sistema de Control Interno generando una cultura de Autocontrol y autoevaluación en materia gestión y valoración de los riesgos al interior de la misma**.**

Colombia cuenta con la Guía de gestión de riesgos (MinTIC, 2016), que se clasifica en tres etapas a saber:

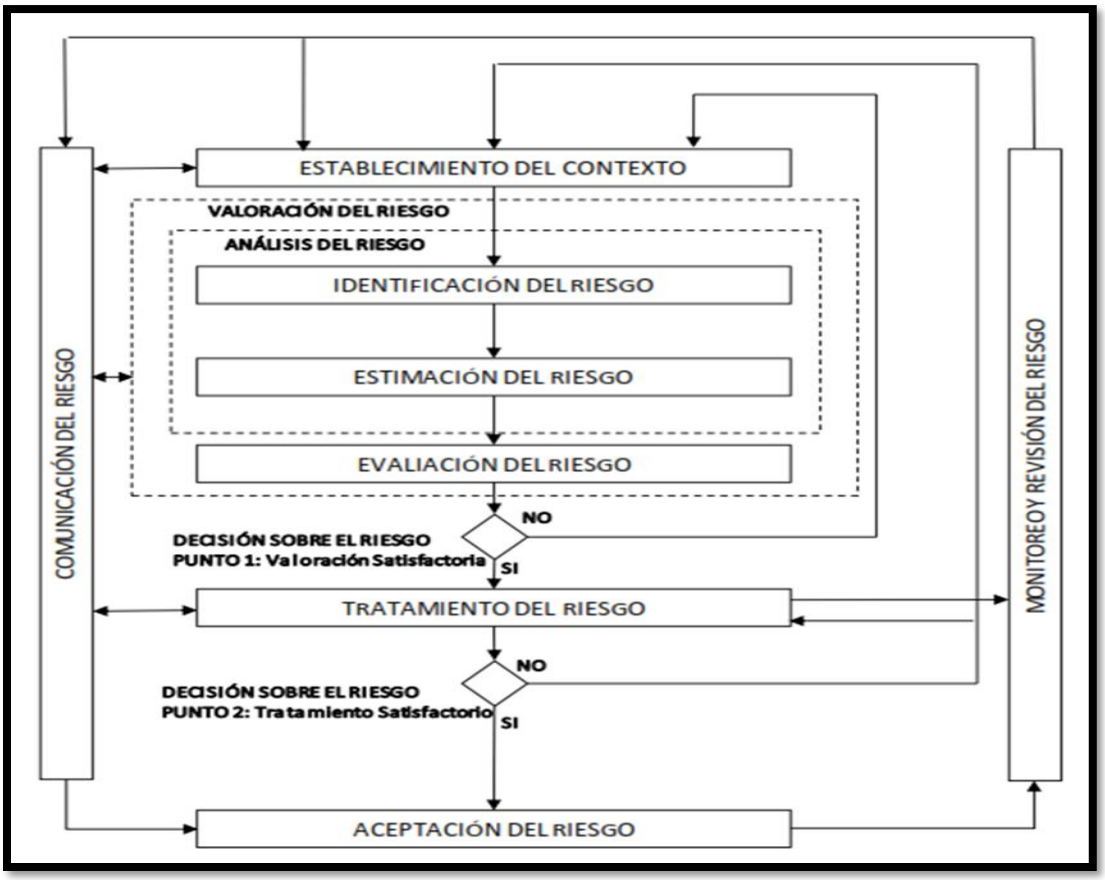
- Compromiso de la alta y mediana dirección, fundamental para la toma de decisiones y aprobación de cada etapa de la gestión de los riesgos.
- Conformar un equipo MECI o de un grupo interdisciplinario, para que diferentes áreas de la organización aporten al tratamiento de los riesgos.
- Capacitación en la metodología, el equipo anterior debe capacitarse para poder realizar análisis de los riesgos de seguridad.

Como lo referencia la norma ISO (2011), para gestionar los riesgos de seguridad de la información se deben tener en cuenta los siguientes pasos: establecer el contexto, identificar el

riesgo, realizar la estimación del riesgo, evaluar el riesgo, tratar el riesgo y aceptar el riesgo, lo anterior se debe socializar a las partes interesadas y realizar un continuo monitoreo y revisión del riesgo para garantizar que este se está controlando dentro de los parámetros aceptados.

En la siguiente figura se representa el proceso para la administración del riesgo:

Figura 1. Proceso para la administración del Riesgo en Seguridad de la Información



Fuente: Norma ISO, (2011)

2.2.4. Metodologías de análisis y gestión de riesgo

A continuación, se relacionan algunas de las metodologías más usadas en la actualidad para realizar el análisis y la gestión de riesgos:

2.2.4.1. Metodología MAGERIT

Para entender esta metodología se requiere entender algunos conceptos como el de seguridad, el cual, según el Gobierno de España, (2012),P.8), lo define como:

> La capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o mal intencionadas que comprometen la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles, (p.8).

Es decir, se busca la manera de blindar las redes de comunicación de datos contra las posibles amenazas naturales o humanas que puedan existir para atentar contra la estabilidad de las mismas.

Los elementos más importantes para el análisis de riesgos, según MAGERIT son: activo, vulnerabilidades, amenaza, impacto, riesgo y salvaguardas (funciones, servicios y mecanismos).

De la misma manera, de acuerdo con MAGERIT, el proceso de análisis de riesgos se desarrolla en las siguientes etapas: planificación, análisis de riesgos, gestión de riesgos y selección de salvaguardas.

MAGERIT detalla su metodología desde tres puntos de vista:

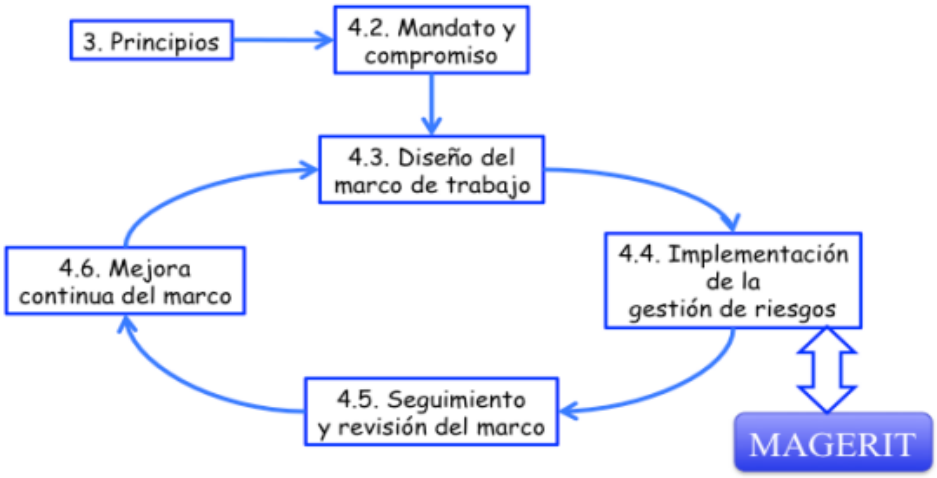
- Detalla los pasos para analizar el estado del riesgo y gestionar su mitigación.
- Detalla las tareas básicas para realizar un proyecto de análisis y gestión de riesgos.
- Visualiza una serie de aspectos prácticos derivados de la experiencia acumulada en el tiempo para analizar y gestionar el riesgo de manera efectiva.

La metodología referida, ayuda a descubrir y planificar medidas eficientes para mantener los riesgos bajo control y apoyar en la preparación de la organización para procesos de evaluación,

auditoría, certificación o acreditación; igualmente, una de sus mayores ventajas es que las decisiones que deban tomarse y que tengan que ser validadas por la alta dirección estarán fundamentadas y serán fácilmente defendibles. Otro aspecto para resaltar se basa en que sus resultados se expresan en valores económicos lo que, a su vez, también es una desventaja por cuanto el hecho de tener que traducir de forma directa todas las valoraciones en valores económicos, hace que la aplicación de esta metodología sea muy costosa.

De acuerdo con lo establecido por la norma ISO 31000, MAGERIT responde a lo denominado "Proceso de Gestión de los Riesgos"; es decir MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías

Figura 2. ISO31000 - Marco de trabajo para Gestionar Riesgos



Fuente: (Gobierno de España, 2012,P.8)

Hay varias formas de analizar los riesgos soportados por los sistemas TIC, como son:

- Guías informales
- Aproximaciones metódicas y
- Herramientas de soporte.

Todas buscan realizar el análisis objetivo de los riesgos para saber qué tan seguros (o inseguros) son los sistemas y no engañarse. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan, pues hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poca fiabilidad.

Según lo establece el Gobierno de España, (2012, p.8), MAGERIT busca que se cumplan los siguientes objetivos:

Directos:

- Que los responsables de las organizaciones tomen conciencia de la existencia de riesgos y de la necesidad de gestionarlos.
- Proveer un método sistemático que permita analizar los riesgos derivados del uso de tecnologías de la información y las comunicaciones (TIC).
- Apoyar para el descubrimiento y planificación para el tratamiento oportuno que permita mantener los riesgos bajo control

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

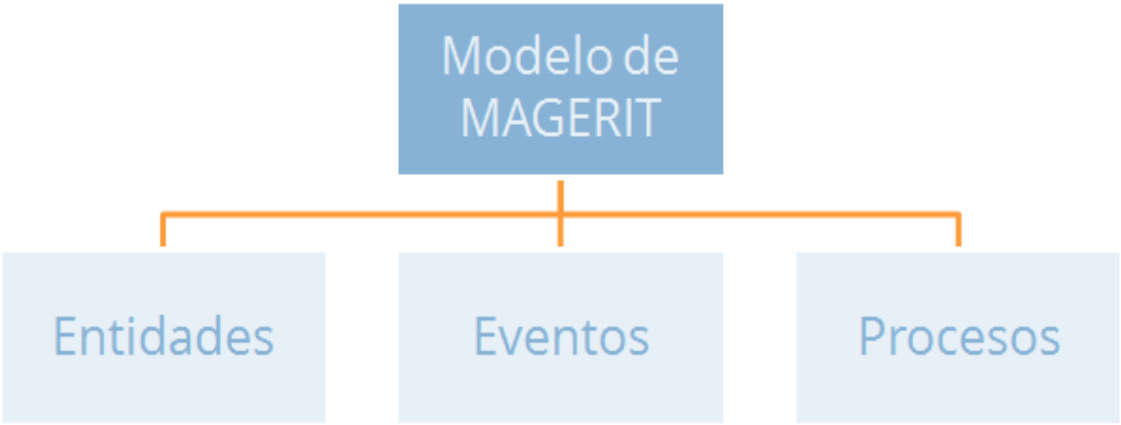
Igualmente se busca la estandarización de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos, destacando lo siguiente:

- Modelo de valor: caracterización de la importancia del valor que representan los activos para la Organización, así como de las dependencias entre los diferentes activos.
- Mapa de riesgos: relación de las diversas amenazas a las cuales están expuestos los activos.

También se destaca en la metodología la declaración de aplicabilidad, la evaluación de salvaguardas, el estado de riesgo, el informe de insuficiencias, cumplimiento de la normativa y plan de seguridad.

MAGERIT presenta una visión estratégica holística de la Seguridad de los Sistemas de Información como lo establece el estándar ISO 27001, el cual inicia con un modelo de análisis y gestión de riesgos que se compone de tres modelos: entidades, eventos y procesos, como se puede observar en la figura 6.

Figura 3. Componentes Modelo MAGERIT



Fuente: PMG, (2018, p1)

2.2.4.2. Octave (Operationally Critical Threat Asset and Vulnerability Evaluation).

Según lo establece el Software Engineering Institute, (2007), OCTAVE es una metodología para identificar y evaluar los riesgos de seguridad de la información, desarrollada por el CERT en Carnegie Mellon University.

La metodología pretende ayudar a las organizaciones a:

- Ser tolerantes al riesgo operacional

• Identificar activos importantes para la misión de la organización

• Identificar vulnerabilidades y amenazas a esos activos

• Determinar y evaluar posibles consecuencias para la organización, en el caso de materializasen las amenazas.

Hay tres métodos de OCTAVE que se basan en la práctica y evaluación de la seguridad que tienen en cuenta la información de riesgo. Estos criterios establecen los principios fundamentales y los atributos de gestión de riesgos que se usan por los métodos de OCTAVE, los cuales son el método OCTAVE, el método OCTAVE-S y el Método OCTAVE ALLEGRO

- ***Método OCTAVE****:* este método se ejecuta en tres fases que examinan el estado de la organización y aspectos tecnológicos, presenta una visión clara de la organización y sus necesidades de información y seguridad de esta. Está compuesta por un conjunto de talleres, facilitados o llevados a cabo por un equipo de análisis interdisciplinario de tres a cinco personas de la misma organización. El método aprovecha el conocimiento de múltiples niveles de la organización, centrándose en:

  - Identificación de los elementos críticos y las amenazas a los activos.
  - Identificación de vulnerabilidades, tanto organizativas y tecnológicas, que exponen a las amenazas, creando un riesgo a la organización.
  - Desarrollo de una estrategia basada en la protección de prácticas y planes de mitigación de riesgos para apoyar la misión de la organización y las prioridades.

  Las actividades anteriores se apoyan de un catálogo de buenas prácticas, encuestas y hojas de cálculo que se puede utilizar para obtener y captar información durante los debates y la solución de problemas.

- ***Método OCTAVE-S*:** cumple con los mismos criterios que el método OCTAVE pero está adaptado a los limitados medios y restricciones únicas de las pequeñas organizaciones. OCTAVE-S utiliza un proceso simplificado y hojas de trabajo diferentes, pero produce el mismo tipo de resultados. Requiere un pequeño equipo de 3-5 personas que entienden la amplitud y profundidad de la empresa. En esta versión se realizan talleres para recopilar información sobre los elementos importantes, las amenazas, requisitos de seguridad y prácticas de seguridad. Esta metodología incluye sólo una exploración limitada de la infraestructura informática. Se parte del supuesto que el equipo de análisis de la información se conoce.

- ***Método OCTAVE ALLEGRO*:** corresponde a una versión derivada y simplificada del método de OCTAVE, la cual se centra en los activos de la información. Esta metodología puede realizar un taller de entorno colaborativo, pero también es muy apropiado para las personas que desean realizar la evaluación de riesgo sin una amplia participación de la organización o experiencia.

OCTAVE ALLEGRO se compone de ocho pasos organizados en cuatro fases:

- Fase 1 – En la cual se evalúan los participantes, desarrollando criterios de medición del riesgo con las directrices de la organización, teniendo en cuenta los objetivos, la misión de la organización y los factores críticos de éxito.
- Fase 2 – Todos los participantes crean un perfil de los activos críticos de información, que establece límites claros para el activo, identifica sus necesidades de seguridad, e identifica todos sus contenedores.
- Fase 3 – Todos los participantes identifican las amenazas que puede sufrir la información de cada activo en el contexto de sus contenedores.

- Fase 4 - Los participantes identifican y analizan los posibles riesgos para los activos de información y desarrollan planes de mitigación.

2.2.4.3. DAFP.

Esta metodología para la administración de riesgos, fue presentada en el año 2009 por el Departamento Administrativo de la Función pública de Colombia (DAFP), tuvo una actualización en el año 2011 y posteriormente en el 2014.

Al respecto el (Departamento Administrativo de la Función Pública, 2014), manifiesta que la administración del riesgo ayuda al conocimiento y mejoramiento de la entidad, a elevar la productividad y a garantizar la eficiencia y la eficacia en los procesos organizacionales, logrando así definir estrategias de mejoramiento continuo, brindándole un manejo sistémico a la entidad.

Por otra parte destaca la importancia de incorporar al interior de las entidades la gestión del riesgo, como una política de gestión por parte de la alta dirección y cuente con la participación y respaldo de todos los servidores públicos; lo anterior se facilitará con la implementación de la metodología, la cual permite establecer mecanismos para valorar , identificar y minimizar los riesgos a los que constantemente están expuestas y poder de esta manera fortalecer el Sistema de Control Interno permitiendo el cumplimiento de los objetivos misionales y los fines esenciales del Estado.

La recomendación antes de iniciar con la implementación es tener claridad sobre el contexto de la entidad (Misión, Visión, Objetivos estratégicos y Planeación institucional), como también identificar la aplicación del modelo de operación por procesos. Posteriormente implementar la metodología con los siguientes tres pasos:

- Paso 1: política de Administración del Riesgo. Identificar qué y cómo puede suceder.

- Paso 2: identificación del riesgo. Definir la probabilidad, las consecuencias y el nivel de riesgo.
- Paso 3: valoración del riesgo. Identificar los controles seleccionados para minimizar y controlar el riesgo, verificar la efectividad de los mismos y establecer el tratamiento de los riesgos.

2.2.4.4. Ebios

(Expresión de las necesidades e identificación de los objetivos de seguridad). Metodología francesa de análisis y gestión de riesgos de seguridad de sistemas de información. Según lo referencia Lopez, (2014), el método EBIOS permite visualizar y dar tratamiento a los riesgos relativos a la seguridad de los sistemas de información (SSI). Mejora la comunicación dentro de la entidad y también con las entidades asociadas para contribuir al proceso de la gestión de los riesgos SSI. Brinda apoyo para la toma de decisiones de la materia y puede utilizarse para numerosas finalidades y procedimientos de seguridad, tales como la elaboración de esquemas directivos, de políticas, de políticas de protección o de objetivos de seguridad, de los planes de acción o de cualquier otra forma de pliego de condiciones de SSI, (p.5).

EBIOS se puede utilizar para el estudio de sistemas por diseñar como también sistemas ya existentes. En el primer caso, permite determinar las especificaciones de seguridad integrándose a la gestión de Proyectos. En el segundo caso, considera las medidas de seguridad existentes e integra la seguridad a los sistemas en funcionamiento.

2.2.5. Sistema de Gestión de Seguridad de la información

Actualmente se tiene como referente en materia de SGSI, la norma ISO/IEC 27001, la cual brinda un modelo para establecer, implementar, operar y realizar seguimiento, revisión y mejora al mismo. Fue publicada en octubre de 2005 y revisada y actualizada el 25 de septiembre de 2013.

La norma ISO 27001, al respecto manifiesta que “Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una política definida, documentada y conocida por todos, que se revisa y mejora constantemente”.

En su anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002, la organización tiene libertad para implementar los controles enumerados en dicho anexo.

La Norma ISO/IEC 27002 (2007), publicada desde el 1 de julio, es una guía de buenas prácticas en la cual se detallan los objetivos de control y los controles recomendados en cuanto a seguridad de la información. Esta norma no es certificable.

La norma NTC- ISO-IEC 27002, se actualizó en el año 2013, cuenta con 14 dominios, 35 objetivos de control y 114 controles, se tradujo al castellano como UNE-ISO/IEC 27002:2015 desde el 1 de julio de 2015.

2.2.6. Modelo de Seguridad y Privacidad de la Información (MSPI)

La construcción del Modelo de Seguridad y Privacidad de la Información (MSPI), fue liderada por el Ministerio de Tecnologías de la Información y Comunicaciones del Gobierno de Colombia, en él se recopilan las mejores prácticas nacionales e internacionales que suministran los elementos necesarios para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo del SGSI, como parte de la estrategia de Gobierno en línea.

El MSPI está alineado con el Marco de referencia de Arquitectura de TI y soporta transversalmente los otros tres componentes de la estrategia GEL como son: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

El MSPI facilita el entendimiento del proceso de construcción de una política de privacidad por parte de la entidad, la cual permite fijar los criterios que se deben aplicar para

proteger la privacidad de la información y los datos, así como también los procesos y las personas vinculadas a la información.

Teniendo en cuenta lo establecido en (MinTIC, 2018), el ciclo de operación del MSPI se compone de las siguientes fases:

- **Fase de Diagnóstico:** se identifica el estado actual o presente de la entidad con respecto a los requerimientos del MSPI, en la siguiente tabla se ilustra las metas, resultados e instrumentos de esta fase:

Tabla 1. Metas, resultados e Instrumentos en el Diagnóstico

Diagnostico			
Metas	**Resultados**	**Instrumentos MSPI**	**Alineación MRAE**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Herramienta de diagnóstico	LI.ES.01 LI.ES.02 LI.GO.01
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Herramienta de diagnóstico	LI.GO.04 LI.GO.05 LI.GO.07

Fuente: (MinTIC, 2018),

- **Fase de Planificación:** en esta fase se elabora el Plan de Seguridad y Privacidad de la información, se alinea con el objetivo misional de la entidad, con el propósito de definir la estrategia y acciones e implementar a través de una metodología de gestión del riesgo, a continuación, se muestran en la siguiente tabla las metas, resultados e instrumentos de esta fase de Planificación:

Tabla 2. Metas, Resultados e Instrumentos Fase de planificación

Planificació			
Metas		**INSTRUMENTOS MSPI**	**MRAE**
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Guía No 2 – Política General MSPI	LI.ES.02 LI.ES.06 LI.ES.07 LI.ES.08
Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Guía no 2 - Política General MSPI	LI.ES.09 LI.ES.10 LI.GO.01 LI.GO.04 LI.GO.07 LI.GO.08 LI.GO.09 LI.GO.10 LI.INF.01 LI.INF.02 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.SIS.22 LI.SIS.23 LI.SIS.01 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12 LI.ST.13 LI.ST.14 LI.UA.01 LI.UA.02 LI.UA.03 LI.UA.04 LI.UA.05 LI.UA.06
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información.	
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.	
Inventario de activos de información.	Documento con la metodología para Identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos	Guía No 5 - Gestión De Activos Guía No 20 - Transición Ipv4 a Ipv6	
Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Guía No 6 - Gestión Documental	
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de Riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la	Guía No 7 - Gestion de Riesgos Guía No 8 - Controles de Seguridad	
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Guía No 14 - Plan de comunicación, sensibilización y capacitación	
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Guía No 20 - Transición IPv4 a IPv6	

Fuente: (MinTIC, 2018)

- **Fase de Implementación:** esta fase le permite a la entidad implementar el Plan de Seguridad y privacidad realizado en la fase anterior, se realiza la Planificación y control operacional, la implementación del plan de Tratamiento de Riesgos y la descripción de los indicadores de gestión.
- **Fase de Evaluación de desempeño:** en esta fase se realiza el monitoreo del Modelo de Seguridad y Privacidad de la Información, con base en los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificar la eficiencia, efectividad y la eficacia de las acciones implementadas. En esta fase se realiza el Plan de revisión y seguimiento a la implementación del MSPI como también el plan de Ejecución de auditorías.
- **Fase de Mejora Continua:** esta fase se consolida los resultados obtenidos en la fase de evaluación de desempeño, para el diseño del Plan de Mejoramiento continuo de seguridad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

Capítulo III. Metodología.

El presente trabajo se desarrolló aplicando el Modelo de Seguridad y Privacidad de la Información (MSPI), que es una guía desarrollada por el Ministerio de Tecnologías de información y Comunicaciones de Colombia, de obligatorio cumplimiento para las entidades públicas del País. En el MSPI se recopilan las mejores prácticas nacionales e internacionales que suministran los elementos necesarios para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo del SGSI, como parte de la estrategia de Gobierno en línea (GEL).

El MSPI facilita el entendimiento del proceso de construcción de una política de privacidad por parte de la entidad, la cual permite fijar los criterios que se deben aplicar para proteger la privacidad de la información y los datos, así como también los procesos y las personas vinculadas a la información.

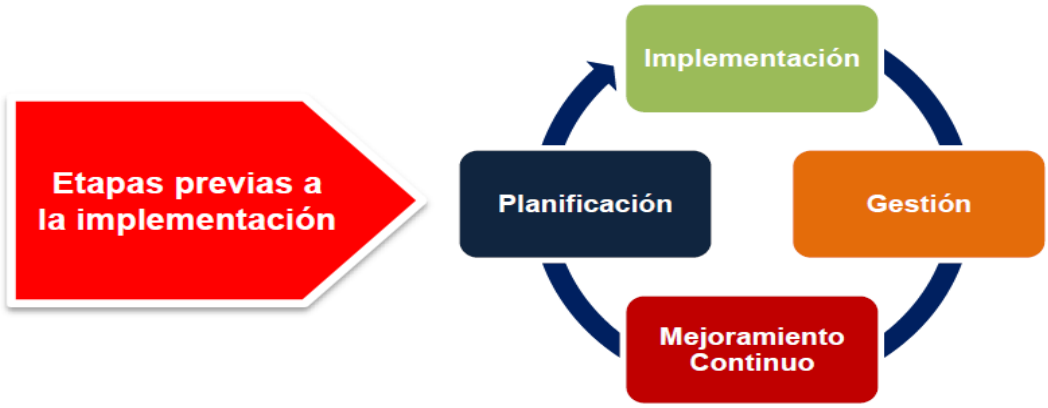
En atención a los objetivos y alcance de este proyecto, como también lo establecido en (MinTIC, 2018), se llevaron a cabo tres fases: diagnóstico, planificación y comunicación.

- **Fase de Diagnóstico:** Se identifica el estado actual o presente de la entidad con respecto a los requerimientos del MSPI.
- **Fase de Planificación**: En esta fase se elabora el Plan de Seguridad y Privacidad de la información, se alinea con el objetivo misional de la entidad, con el propósito de definir la estrategia y acciones e implementar a través de una metodología de gestión del riesgo. Para llevar a cabo el proyecto se aplicó el modelo de seguridad de la información de Gobierno en línea de Colombia, como también las mejores prácticas de hacking ético. Este último tiene como principio usar los conocimientos profesionales en informática y seguridad, para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño. Uno de los conceptos fundamentales de este documento es el de seguridad y privacidad de

la información educativa, que busca que las entidades les garanticen a los ciudadanos que sus datos son tratados como un tesoro, que puedan garantizar la seguridad y privacidad de la información a la hora de hacer trámites y servicios con el Estado (MinTic, 2015, p.1).

Se aplicó la metodología establecida por el modelo de seguridad y privacidad de la información de la estrategia de gobierno en línea de Colombia, en las fases previas a la implementación y planeación.

Figura 4. Marco de seguridad y privacidad de la información



Fuente: *(*MinTIC, 2018, p1)

3.1. Etapas previas a la implementación.

Se identificó el estado actual de la secretaría de Educación del Municipio de Yumbo en materias de seguridad y privacidad de información, el nivel de madurez para lo cual se realizó el respectivo levantamiento de información, lo cual representa la siguiente figura:

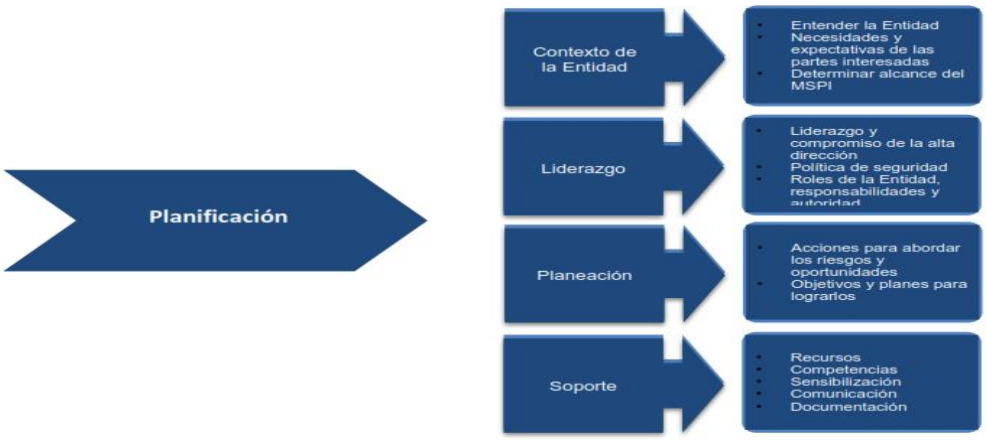
Figura 5. Etapas previas a la implementación

Fuente: (MinTIC, 2018. p.1)

3.2. Etapa de Planificación

Tomando como base los resultados de la etapa anterior se procedió a elaborar el plan de seguridad y privacidad de la información, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información a través de una metodología de gestión del riesgo, lo cual se representa en la siguiente figura**:**

Figura 6. Fase de Planificación



Fuente: (MinTIC, 2018, p1).

3.3. Población y muestra

La población para este estudio estuvo conformada por todos los funcionarios que laboran en la Secretaría de Educación del Municipio de Yumbo, ya que todos producen, gestionan o hacen uso de información y de activos informáticos**.**

Considerando que todos los usuarios no tienen igual responsabilidad ni el conocimiento sobre la información de la institución y la seguridad de la misma, se opta por una muestra intencionada o no probabilística que se selecciona a criterio del investigador según la contribución que puedan hacer al desarrollo del Proyecto. La muestra fue conformada por:

- Secretario de Educación de Yumbo
- Líder TIC del Municipio de Yumbo
- Líder TIC de la Secretaría de Educación
- Líder MECI del Municipio de Yumbo

Técnicas e instrumentos de recolección de datos

Para el desarrollo del presente Proyecto se utilizaron las siguientes técnicas de recolección de información.

- Entrevistas exhaustivas
- Observación.
- Revisión de archivos.
- Sesiones de grupos.

Los instrumentos utilizados para la recolección de datos fueron:

- Herramienta de Diagnóstico. A través del diligenciamiento de esta hoja electrónica, se pudo conocer la realidad de la información relacionada con el manejo de la seguridad y privacidad de los activos de información

- Guía No. 1 – Metodología de pruebas de efectividad: Permite comprobar o medir el nivel de eficiencia de la implementación del modelo de seguridad en la entidad.
- Guía No. 2 – Política General MSPI: Manual con las políticas de seguridad y privacidad de la información.
- Guía No. 3 – Procedimientos de Seguridad y Privacidad de Información: Se refiere a la elaboración documentada de los procedimientos.
- Guía No. 4 – Roles y responsabilidades de seguridad y privacidad de la información: Propuesta de acto administrativo en donde se incluyan los temas de seguridad de la información de la entidad.
- Guía No. 5 – Gestión de Activos: Permite diseñar la matriz con la identificación, valoración y clasificación de los activos de información.
- Guía No. 7 – Gestión de Riesgos: Permite aplicar metodología de gestión de riesgos, análisis y evaluación de riesgos, plan de tratamiento de riesgos y declaración de aplicabilidad.
- Guía No. 8 – Controles de seguridad: Permite seleccionar los controles a aplicar basados en la norma ISO 27002.
- Guía No. 14 – Plan de comunicación, sensibilización y capacitación: Permite elaborar el plan de comunicación, sensibilización y capacitación de la entidad.

Al finalizar el proyecto se logró aplicar todos los instrumentos lo que conllevó a la elaboración del Plan de Seguridad y Privacidad.

Teniendo en cuenta lo anterior se procedió a diligenciar la herramienta diagnóstica, la cual permite obtener un resultado preciso sobre la situación actual de la Secretaría de Educación del Municipio de Yumbo en esta materia y que servirá de base para generar el Plan de Seguridad de

la Información, propósito del presente proyecto, para este propósito, se realizaron reuniones con diferentes actores que intervienen de alguna manera con la seguridad de la información que se describen a continuación:

Tabla 3. Responsables y áreas involucradas

RESPONSABLE	**RESPONSABILIDAD**
Responsable de la seguridad física	SEGURIDAD FÍSICA Y DEL ENTORNO
	ÁREAS SEGURAS
	Perímetro de seguridad física
	Áreas de despacho y carga
	Visita al Centro de Computo
Responsable de SI	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN
	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
	SEGURIDAD DE LOS RECURSOS HUMANOS
	Antes de asumir el empleo
	Durante la ejecución del empleo
	Terminación y cambio de empleo
	GESTIÓN DE ACTIVOS
	CUMPLIMIENTO
Responsable de Si	**POLICAS DE SEGURIDAD DE LA INFORMACIÓN**
	Cumplimiento de requisitos legales y contractuales
	CONTROL DE ACCESO
	CRIPTOGRAFÍA
	SEGURIDAD FÍSICA Y DEL ENTORNO
	SEGURIDAD DE LAS OPERACIONES

RESPONSABLE	RESPONSABILIDAD
	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES
	Procedimientos de operación documentados
	Gestión de cambios
	Gestión de capacidad
	Separación de los ambientes de desarrollo, pruebas y operación
	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS
	COPIAS DE RESPALDO
	REGISTRO Y SEGUIMIENTO
	Registro de eventos
	Protección de la información de registro
	Registros del administrador y del operador
	Sincronización de relojes
	CONTROL DE SOFTWARE OPERACIONAL
	Instalación de software en sistemas operativos
	GESTIÓN DE LA VULNERABILIDAD TÉCNICA
	Gestión de las vulnerabilidades técnicas
	Restricciones sobre la instalación de software
Responsable de Si	**POLICAS DE SEGURIDAD DE LA INFORMACIÓN**
	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN
	Controles sobre auditorías de sistemas de información
	SEGURIDAD DE LAS COMUNICACIONES
	GESTIÓN DE LA SEGURIDAD DE LAS REDES

RESPONSABLE	RESPONSABILIDAD
	TRANSFERENCIA DE INFORMACIÓN
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN
	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE
	DATOS DE PRUEBA
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
	Alcance MSPI (Modelo de Seguridad y Privacidad de la Información)
	Identificación y valoración de riesgos
	Tratamiento de riesgos de seguridad de la información
	Toma de conciencia, educación y formación en la seguridad de la información
	Planificación y control operacional
	Implementación del plan de tratamiento de riesgos
	Indicadores de gestión del MSPI
	Plan de seguimiento, evaluación y análisis del MSPI
	Evaluación del plan de tratamiento de riesgos
	Plan de seguimiento, evaluación y análisis del MSPI
Responsable de Si	**POLICAS DE SEGURIDAD DE LA INFORMACIÓN**
	Tratamiento de temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, o en los comités directivos interdisciplinarios de la Entidad

RESPONSABLE	RESPONSABILIDAD
	Con base en el inventario de activos de información clasificado, se establece la caracterización de cada uno de los sistemas de información.
	La entidad conoce su papel dentro del Estado Colombiano, identifica y comunica a las partes interesadas la infraestructura crítica.
	Las prioridades relacionadas con la misión, objetivos y actividades de la Entidad son establecidas y comunicadas.
	La gestión de riesgos tiene en cuenta los riesgos de ciberseguridad
	Detección de actividades anómalas
	Respuesta a incidentes de ciberseguridad, planes de recuperación y restauración
Responsable de TIC	Teletrabajo
	Manejo de medios
	Derechos de propiedad intelectual.
	CONTROL DE ACCESO
	SEGURIDAD DE LAS OPERACIONES
	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES
	COPIAS DE RESPALDO
	CONTROL DE SOFTWARE OPERACIONAL
	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN
	SEGURIDAD DE LAS COMUNICACIONES
Responsable TIC	GESTIÓN DE LA SEGURIDAD DE LAS REDES
	TRANSFERENCIA DE INFORMACIÓN
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

RESPONSABLE	RESPONSABILIDAD
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
	Plan y Estrategia de transición de IPv4 a IPv6
	Implementación del plan de estrategia de transición de IPv4 a IPv6
	Redundancias
Calidad	Procedimientos de control documental del MSPI

Fuente: Elaborada bajo la referencia de MinTIC, (2017)

Capítulo IV. Estado actual de la gestión de seguridad de la información en la Secretaría de Educación del Municipio de Yumbo.

En las reuniones de trabajo se solicita y consolida información de seguridad y privacidad de la información, se realizan pruebas administrativas, técnicas, análisis del avance del ciclo PHVA y análisis frente a las mejores prácticas y luego se diligencia la herramienta diagnóstica.

Se inicia el proceso de diligenciamiento de la herramienta con los datos de la portada, en donde se registran los datos de la entidad evaluada, fechas de evaluación, contacto y datos de quien elabora la herramienta, lo anterior se evidencia en la siguiente figura:

Figura 7. Datos Básicos Portada

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN / MINTIC	INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD HOJA PORTADA	vive digital para la gente
ENTIDAD EVALUADA	ALCALDÍA MUNICIPAL DE YUMBO - SECRETARIA DE EDUCACIÓN	
FECHAS DE EVALUACIÓN	16/07/2018 a 31/08/2018	
CONTACTO	Hames Vargas Polanco - Líder TIC SEMY - hamesv@yumbo.gov.co; hamesvargas@hotmail.com	
ELABORADO POR	Hames Vargas Polanco.	

Fuente: elaboración propia

Seguidamente se procede a analizar los resultados de la evaluación de efectividad de controles ISO-27001:2013 Anexo A. En la hoja de trabajo denominada **Administrativas**, se realiza el levantamiento de información digitando las pruebas, evidencias, brechas y calificando el nivel de cumplimiento del anexo A ISO 27001 teniendo en cuenta la Tabla de Escala de Valoración de Controles, que se ilustra a continuación:

Tabla 4. Escala de Valoración de Controles ISO 27001

Tabla de Escala de Valoración de Controles

ISO 27001:2013 ANEXO A

Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Fuente: MinTIC, (2017)

Una vez definida la escala de valoración de controles, se procedió a documentar el análisis sobre la situación actual en materia de seguridad y privacidad de la información del Municipio de Yumbo:

4.1. Políticas de seguridad de la información (control a.5)

Este control orienta sobre la dirección para gestión de la seguridad de la información.

Se solicita al líder TIC de la Alcaldía de Yumbo si existe una política de seguridad de la información para evaluar:

a) Si se definen los objetivos, alcance de la política

b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad (Inexistencia absoluta del documento)

c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección.

El Ingeniero líder TIC manifiesta que no existe una política de seguridad y privacidad de la información, por lo anterior se asigna una calificación de **Cero (0)**, correspondiente a una evaluación de efectividad de control **Inexistente**, lo que conlleva a la necesidad de elaborar la

política de seguridad y privacidad de la información, aprobada y firmada, como también la revisión y actualización periódica de la misma.

4.2. Organización de la seguridad de la información (Control A.6)

Este control sirve como marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización, como también garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles.

Se verifica que no se ha adelantado mucho en este aspecto por las siguientes razones:

- los roles y responsabilidades frente a la ciberseguridad no han sido establecidos.
- los roles y responsabilidades de seguridad de la información no han sido coordinados y alineados con los roles internos y las terceras partes externas.
- No están claros los roles y responsabilidades para la detección de incidentes.
- No existe un acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información, revisado y aprobado por la alta Dirección.

No existe un Sistema de Gestión de la Seguridad de la Información, por lo tanto.

1) Actualmente no hay suficiente apoyo de la alta dirección para discutir temas como la política de Seguridad de la Información, los riesgos o incidentes.

2) No están claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas, en materia de SI.

3) Si están identificados los responsables y responsabilidades para la protección de los activos, actualmente se nombra un responsable para cada activo quien se encarga de su protección.

4) No están definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales.

5) Sí están definidos, pero no documentados los niveles de autorización, por políticas de directorio activo de Windows server.

6) No se cuenta con un presupuesto formalmente asignado a las actividades del SGSI, no se hacen campañas de sensibilización en seguridad de la información.

Se evidencia que los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores; Por lo anterior se asigna una calificación de **Treinta (30)**, correspondiente a una evaluación de efectividad de control **Repetible**, lo que implica la necesidad de que:

1) Se deben establecer los roles y responsabilidades frente a la ciberseguridad.
2) Se debe coordinar y alinear los roles y responsabilidades de seguridad de la información con los roles internos y las terceras partes externas.
3) Se debe capacitar a las partes interesadas de la secretaría de educación los roles y responsabilidades para la detección de incidentes.
4) Documentar procesos y procedimientos.
5) Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. Por ejemplo, a través de una membresía.

6) Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
7) Se deben establecer procedimientos que especifiquen cuándo y a través de que se debe contactar a las autoridades (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de reglamentación y las autoridades de supervisión), y cómo se debe reportar de una manera oportuna los incidentes de seguridad de la información identificados (por ejemplo, si se sospecha una violación de la ley).
8) Se debe Integrar la seguridad de la información en el ciclo de vida de los proyectos.
9) Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
10) Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo. (para ello revisar libro blanco de teletrabajo).

4.3. Seguridad de los recursos humanos (Control A.7)

La norma establece que “las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos”. (MinTIC, 2016)

Al respecto se verifica que no se ha adelantado mucho en este aspecto por las siguientes razones:

1) La contratación se realiza por etapas, una etapa preliminar donde se atiende la solicitud dependiendo de las necesidades de un área específica, luego se realiza un

seguimiento para la recolección de los datos, la información y la documentación necesaria, después se escala con el personal de recursos humanos y encargados para asignar las actividades, finalmente se realiza la contratación. Se aplica la ley 80 de contratación.

2) Los acuerdos contractuales con empleados y contratistas, no establecen responsabilidades en cuanto a la seguridad de la información.

Por lo anterior se asigna una calificación de **Treinta y Uno (31)** correspondiente a una evaluación de efectividad de control **Repetible**, lo que implica la necesidad de que se ajuste el proceso de contratación y se incorpore en los contratos responsabilidades en cuanto a la seguridad de la información.

4.4. Gestión de activos (Control Número A.8)

Este control busca que se identifiquen los activos organizacionales y definir las responsabilidades de protección apropiadas.

En este sentido se encuentra que el Municipio de Yumbo cuenta con un software de inventario llamado SRF PLUS, en donde se registran todos los activos de la administración, también manejan un inventario manual, y marcan todos estos con placas, la Secretaria de Gestión Humana y Recursos Físicos se encarga de administrar los inventarios.

Por lo anterior se asigna una calificación de **Cincuenta y Ocho (58)** correspondiente a una evaluación de efectividad de control **Efectivo**, lo que implica la necesidad de que se realicen las siguientes actividades:

1) Desarrollar el procedimiento mediante el cual se clasifican, se etiquetan y manejan los activos de información.

2) Documentar guías, lineamientos y procedimientos para la gestión de medios removibles.
3) Desarrollar directrices para la protección de medios físicos.

4.5. Control de acceso (Control A.9)

Este control indica que se debe limitar el acceso a la información y a las instalaciones de procesamiento de información, para ello se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

Se evidencia que en el Municipio de Yumbo esta implementado directorio activo y servidor de bases de datos con usuarios creados y seleccionados con sus perfiles y roles, para acceso a los sistemas de información de la Alcaldía y Secretaría de Educación, pero falta documentar la política de control de acceso y revisar la manera de asignar claves de administrador.

Por lo anterior se asigna una calificación de **Sesenta y Seis (66)** correspondiente a una evaluación de efectividad de control **Gestionado**, lo que implica la necesidad de que se realicen las siguientes actividades:

1) Crear política de control de acceso.
2) Revisar y ajustar asignación de claves a usuarios.

4.6. Criptografía (Control A.10)

Este control permite asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y la integridad de la información.

En el levantamiento de información se pudo evidenciar que no existe una política sobre el uso de controles criptográficos para la protección de la información de los datos tributarios (Pagos) en el aplicativo Impuestos Pluss.

Por lo anterior se asigna una calificación de **Cero (0)** correspondiente a una evaluación de efectividad de control **Inexistente**, lo que implica la necesidad de que se realicen las siguientes actividades:

1) Se debe evaluar la posibilidad de desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
2) Se debe evaluar la posibilidad de desarrollar.

4.7. Seguridad física y del entorno (Control A.11)

Este control permite prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

Se pudo evidenciar que actualmente no existen directrices relacionadas con los perímetros de seguridad física, el acceso al DataCenter se da mediante tarjeta de acceso y solo a personal autorizado, hay Seguridad Física con vigilancia privada y cámaras IP, falta identificar el DataCenter, no se identifican los elementos de resiliencia, no existe procedimiento para revisar trabajo en área segura, el Área de carga, descarga y despacho a cargo de operarios y del almacén el cual se encuentra ubicado externo a las instalaciones de la Alcaldía de Yumbo.

Por lo anterior se asigna una calificación de **Treinta y Nueve (39)** correspondiente a una evaluación de efectividad de control **Repetible**, lo que implica la necesidad de que se realicen las siguientes actividades:

1) Crear directrices relacionadas con los perímetros de seguridad física.
2) Identificar DataCenter.
3) Identificar los elementos de resiliencia.
4) Crear procedimiento para revisar trabajo en área segura.
5) Actualizar y adecuar Datacenter.

6) Programar mantenimiento preventivo de equipos de cómputo.
7) Crear procedimiento para retiro y devolución de equipos de cómputo de las instalaciones de la Alcaldía.
8) Crear procedimiento para transporte de equipos de cómputo.
9) Crear proceso de borrado de discos y de encriptación del disco.
10) Crear procedimiento equipos de usuarios desatendidos.
11) Crear directrices para escritorio limpio.

4.8. Seguridad de las operaciones (Control A.12)

En este control se realizan las siguientes evidencias:

1) Las aplicaciones de misión crítica de la Alcaldía y de la secretaria de Educación de Yumbo son tercerizadas y se aplica claramente la gestión de cambios, sin embargo, no existe documentación al respecto.
2) No existe procedimiento para gestionar la demanda de capacidad.
3) No existe procedimiento para la separación de ambientes.
4) No existe política formal para el uso de software no autorizado.
5) Si existe una solución de antivirus (Sophos).
6) Existen log que se generan a través de Directorio Activo, falta hacerle seguimiento a los mismos regularmente.
7) No existen procedimientos y controles dirigidos a proteger contra cambios no autorizados de la información de registro.
8) Los relojes de sistema se sincronizan con Directorio Activo de Windows server implementado.

Por lo anterior se asigna una calificación de **Treinta y Ocho (38)** correspondiente a una evaluación de efectividad de control **Repetible**, lo que implica la necesidad de que se realicen las siguientes actividades:

1) Documentar la gestión de cambios.
2) Crear procedimiento para gestionar la demanda de capacidad.
3) Crear procedimiento para la separación de ambientes.
4) Crear política formal para el uso de software no autorizado.
5) Hacerle seguimiento a los log´s que se generan a través de Directorio Activo regularmente.
6) Crear procedimientos y controles dirigidos a proteger contra cambios no autorizados de la información de registro.

4.9. Seguridad de las comunicaciones (Control A.13)

Se encuentra como evidencia que se gestiona el acceso a las redes de forma *ad hoc*, es decir basados en el conocimiento y experiencia de los ingenieros de sistemas adscritos al Departamento Administrativo de Planeación e Informática, lo anterior indica que no existen directrices para la gestión de seguridad de redes, tampoco para la seguridad de los servicios de red, están parcialmente implementadas VLAN y GPO, no existen Políticas y procedimientos de transferencia de información, no existen acuerdos sobre transferencia de información, no existen directrices para mensajería electrónica (se maneja a través de un tercero la mensajería corporativa EMCALI), no existen acuerdos de confidencialidad (se referencian tangencialmente en contrato laboral).

Por lo anterior se asigna una calificación de **Treinta y Siete (37)** correspondiente a una evaluación de efectividad de control **Repetible**, lo que implica la necesidad de que se realicen las siguientes actividades:

1) Crear directrices para la gestión de seguridad de redes.
2) Crear directrices para la seguridad de los servicios de red.
3) Crear e implementar VLAN y GPO.
4) Crear políticas y procedimientos de transferencia de información.
5) Realizar acuerdos sobre transferencia de información.
6) Crear directrices para mensajería electrónica.
7) Implementar acuerdos de confidencialidad en los contratos laborales.

4.10. Adquisición, desarrollo y mantenimiento de sistemas (Control A.14)

Este control permite que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.

En la actualidad la alcaldía de Yumbo tiene contratado el soporte y actualización de los sistemas de información tributario, financiero, inventarios y nómina.

Se encuentran las siguientes evidencias para este control:

1) No existen directrices para análisis y especificaciones de requisitos de seguridad de la información.
2) No existen directrices para la seguridad de servicios de las aplicaciones en redes públicas (sin embargo, esta implementado parcialmente un firewall físico para control de acceso remoto y configuración de listas de acceso).

3) No existen directrices para la protección de transacciones de los servicios de las aplicaciones.
4) No existe una política de desarrollo de software seguro (se desarrolla software eventualmente ad hoc).
5) No existen procedimientos de control de cambios en sistemas (se realizan ad hoc).
6) Se revisan las aplicaciones, pero no hay directrices formalmente establecidas.
7) No existen directrices para los cambios a los paquetes de software.
8) No se han establecido Principios de construcción de sistemas seguros.
9) No se han establecido directrices para ambiente de desarrollo seguro.
10) Se supervisa y hace seguimiento de la actividad de desarrollo de sistemas contratados externamente Nómina, Impuestos, sistema financiero y sistema de recursos físicos.
11) No se realizan pruebas de seguridad de sistemas.
12) Se realizan las pruebas de aceptación, pero sin dejarlas documentadas.
13) No se realiza protección de datos de prueba.

Por lo anterior se asigna una calificación de **Quince (15)** correspondiente a una evaluación de efectividad de control **Inicial**, lo que indica que:

1) Hay una evidencia de que la organización ha reconocido que existe un problema y que hay que tratarlo.
2) No hay procesos estandarizados.
3) La implementación de un control depende de cada individuo y es principalmente reactiva.
4) Se cuenta con algunos procedimientos documentados, pero no son conocidos y/o no se aplican.

Lo anterior implica la necesidad de que se realicen las siguientes actividades:

1) Crear directrices para análisis y especificaciones de requisitos de seguridad de la información.
2) Crear directrices para la protección de transacciones de los servicios de las aplicaciones.
3) Crear política de desarrollo de software seguro.
4) Crear procedimientos de control de cambios en sistemas.
5) Crear directrices para revisión técnica de las aplicaciones después de cambios en la plataforma de operación.
6) Crear directrices restricciones en los cambios a los paquetes de software.
7) Definir principios de construcción de sistemas seguros.
8) Crear directrices para ambiente de desarrollo seguro.
9) Documentar la forma de supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
10) Realizar pruebas de seguridad de sistemas.
11) Documentar las pruebas de aceptación.
12) Realizar protección de datos de prueba.

4.11. Relaciones con los proveedores (Control A.15)

En este control se evidencia que no existe una política de seguridad de la información para las relaciones con los proveedores, en la contratación se aplica lo establecido en la ley de contratación estatal (ley 80), se solicitan pólizas de garantía y cumplimiento que son verificados por supervisores de contrato.

Por lo anterior se asigna una calificación de **Cuarenta (40)** correspondiente a una evaluación de efectividad de control **Repetible**, lo que indica que se requiere:

1) Elaborar política de seguridad de la información para las relaciones con los proveedores.

2) Mantener el nivel concertado para la seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

4.12. Gestión de incidentes de seguridad de la información (Control A.16)

Este control permite asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Se evidencia que:

1) Existe una herramienta para mesa de ayuda, pero no están establecidos los procedimientos para la planificación y preparación de respuesta a incidentes.
2) No existen directrices para el reporte de eventos de seguridad de la información, pero se registran automáticamente en *help desk*, directorio activo y solución antivirus.
3) No existen reportes de debilidades de seguridad de la información.
4) No se realiza evaluación de eventos de seguridad de la información y decisiones sobre ellos.
5) No existen procedimientos documentados para dar respuesta a los incidentes de seguridad de la información.
6) No existen planes de respuesta a los incidentes de Seguridad de la Información.
7) No se han definido ni aplicado procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

Por lo anterior se asigna una calificación de **Diez y Siete (17)** correspondiente a una evaluación de efectividad de control **Inicial**, lo que indica que se requiere:

1) Crear procedimientos para la planificación y preparación de respuesta a incidentes,
2) Crear directrices para el reporte de eventos de seguridad de la información.

3) Crear reporte de debilidades de seguridad de la información.
4) Realizar evaluación de eventos de seguridad de la información y decisiones sobre ellos.
5) Crear procedimientos para dar respuesta a los incidentes de seguridad de la información.
6) Crear planes de respuesta a los incidentes de seguridad de la información.
7) Crear directrices para recolección de evidencia.

4.13. Aspectos de seguridad de la información de la gestión de la continuidad del negocio (Control A.17)

Se evidencia que la entidad no cuenta con un BCP (Bussines Continuity Plan) o DRP (Disaster Recovery Plan). Actualmente se cuenta con personal encargado de la seguridad, soporte y mantenimiento de equipos y sistemas de información, pero es personal por contrato de prestación de servicios, no existen planes aprobados, procedimientos de respuesta y recuperación documentados. Se cuenta con procesos pequeños para la realización de pruebas (Como algunas bases de datos de pruebas y algunos servicios de pruebas).

Por lo anterior se asigna una calificación de **Treinta (30)** correspondiente a una evaluación de efectividad de control **Repetible**, lo que indica que se requiere:

1) Desarrollar e implementar el BCP (Bussines Continuity Plan) o DRP (Disaster Recovery Plan).
2) Desarrollar y documentar planes aprobados, procedimientos de respuesta y recuperación.
3) Ampliar pruebas de funcionalidad de procesos, procedimientos y controles de continuidad.
4) Implementar arquitecturas redundantes.

4.14. Cumplimiento (Control A.18)

Este control permite evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

Se evidencia que:

Se aplica la ley 80 de contratación, para su cumplimiento interactúan la oficina de gestión humana, control interno y control interno disciplinario.

No existe política publicada sobre el cumplimiento de propiedad intelectual que defina el uso del software y de productos informáticos.

Existen y están definidas las tablas de retención documental.

1) No existen disposiciones que ha definido la Entidad para cumplir con la legislación de privacidad de los datos personales.
2) No existe Plan de auditorías de seguridad de la información.
3) No existen políticas y normas de seguridad establecidas.
4) Inexistencia absoluta de procedimientos, políticas y normas de seguridad.

Por lo anterior se asigna una calificación de **Veinte (20)** correspondiente a una evaluación de efectividad de control **Inicial**, lo que indica que se requiere:

1) Construir la política sobre el cumplimiento de propiedad intelectual que defina el uso del software y de productos informáticos.
2) Actualizar las Tablas de Retención Documental.
3) Crear disposiciones para cumplir con la legislación de privacidad de los datos personales.
4) Elaborar Plan de Auditorías de seguridad de la información.

5) Desarrollar y establecer políticas y normas de seguridad.

6) Elaborar procedimientos, políticas o normas de seguridad.

En resumen y promediando el puntaje dado sobre la situación actual en materia de efectividad de los controles se cuenta con una calificación de **Treinta (30)** puntos, lo que conlleva a una evaluación de efectividad de controles de **Repetible**, indicando ello que en la Secretaría de Educación del Municipio de Yumbo, los procesos y los controles siguen un patrón regular; los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas, no hay formación ni comunicación formal sobre los procedimientos y estándares y hay un alto grado de confianza en los conocimientos de cada persona, por eso hay alta probabilidad de errores, lo anterior se representa a continuación:

Figura 8. Evaluación de Efectividad de Controles - ISO 27001:2013 Anexo 1

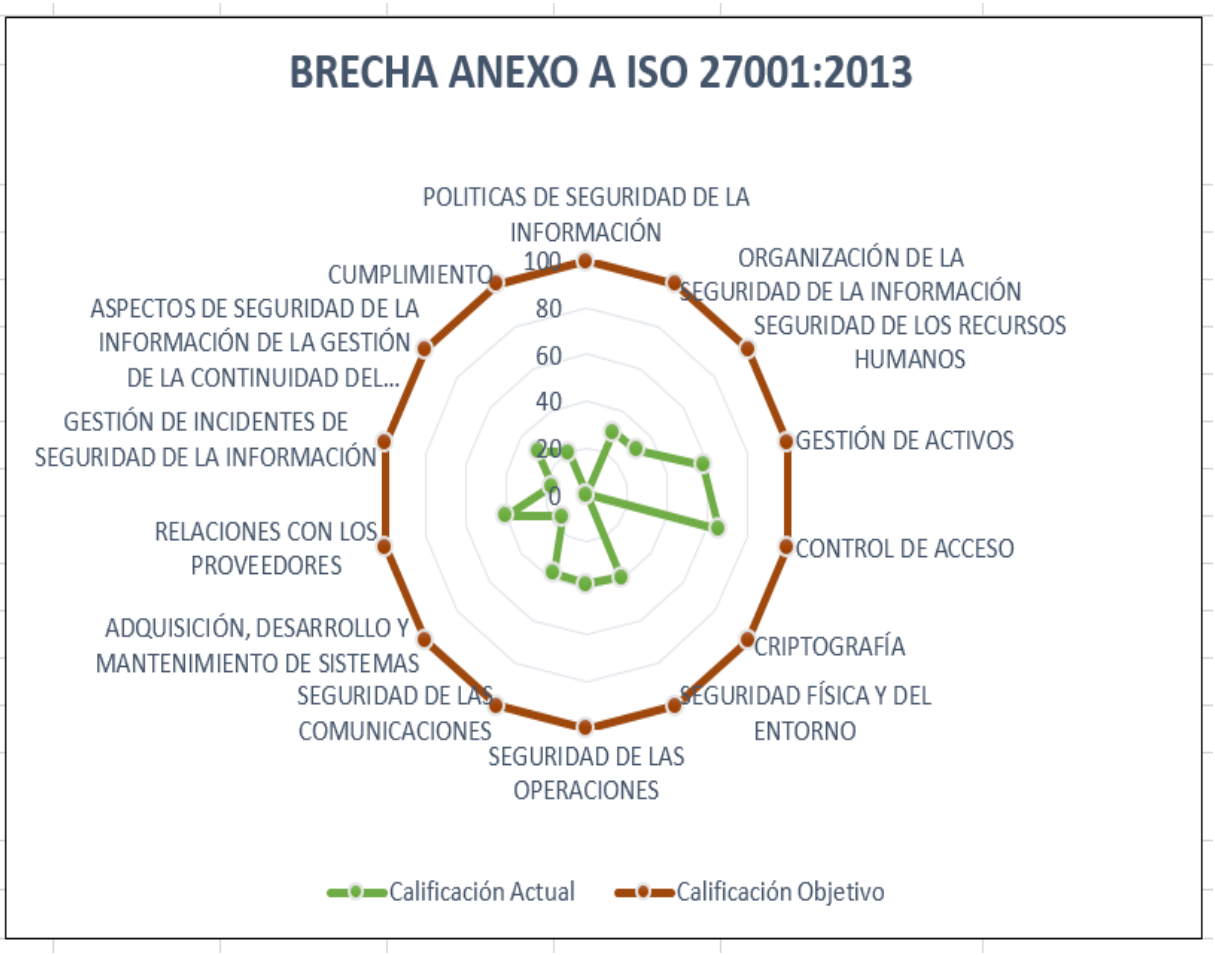
No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	30	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	31	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	58	100	EFECTIVO
A.9	CONTROL DE ACCESO	66	100	GESTIONADO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	39	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	38	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	37	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	15	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	40	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	17	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	100	REPETIBLE
A.18	CUMPLIMIENTO	20	100	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		**30**	**100**	REPETIBLE

Fuente: Elaborado bajo la referencia MinTIC, (2017)

Complementando lo anterior, en la figura 9, se representa la Brecha que hay para cada uno de los controles entre la calificación actual y la calificación objetivo, lo que reitera que se

requiere diseñar e implementar un SGSI y por ende un plan de seguridad que permita reducir la brecha.

Figura 9. Brecha Anexo 1 ISO 27001:2013



Fuente: Elaborado bajo la referenica (MinTIC, (2017)

Capítulo V. Plan de seguridad y privacidad de la información

Para el desarrollo de esta fase se utilizan los resultados de la fase de Diagnostico (ver Anexo1)

- Instrumento_Evaluación_MSPI_Yumbo, procediendo a la construcción del Plan de Seguridad y Privacidad de la Información, el cual se alinea con el objetivo Misional de la Alcaldía de Yumbo y por ende de la Secretaría de Educación Municipal, en este se propone un conjunto de acciones que se deben implementar a nivel de seguridad y privacidad de la información, a través de la metodología establecida por el Modelo de Seguridad y Privacidad de la Información del MInTIC (MSPI).

5.1. Inventario de activos de información

Se refiere a la elaboración de una matriz con la identificación, valoración y clasificación de activos de información. Para realizar esta actividad se toma como referencia la Guía No. 5 – Gestión de Activos, disponible en (MinTIC, 2016).

5.1.1 Inventario de recursos tecnológicos y humanos

En la tabla No. 10 se relacionan los recursos tecnológicos y humanos existentes en la entidad:

5.2 Identificación, valoración y tratamiento de riesgo

La información es parte fundamental y dinámica que mueve a las empresas, después de los seres humanos se convierte en el factor más importante, es por ello que la seguridad se convierte en un factor fundamental para salvaguardar y proteger la información de la entidad minimizando las vulnerabilidades que permitan ser accedidos por delincuentes informáticos.

En este documento se realiza la Identificación, Valoración y Tratamiento de Riesgos para la Secretaría de Educación del Municipio de Yumbo y siguiendo la metodología

propuesta por el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de Información y Comunicaciones de Colombia (MinTIC), se utilizarán como referencias bibliográficas los siguientes documentos:

- La Guía No. 7 – Gestión de Riesgos, disponible en (MinTIC, 2016).
- La Guía No. 8 – Controles de seguridad, disponible en (MinTIC, 2016).
- La Guía de Gestión del Riego del DAFP, disponible en (Departamento Administrativo de la Función Pública (DAFP), 2011)
- Guía para la Gestión y Clasificación de Activos de Información, disponible en (MinTIC, 2016)

5.2.1 Contexto estratégico

5.2.1.1 Actividad específica

El Municipio de Yumbo hace parte de los 42 municipios del Departamento del Valle del cauca, tiene categoría uno, ciento catorce mil (114.000) habitantes, más de dos mil ochocientas (2,800) empresas (Por eso se le denomina como capital Industrial del Valle del Cauca), con un presupuesto de ingresos para la vigencia 2018 que asciende a $282.758.626.981, fuente (Municipio de Yumbo, 2017) y está dentro de sus deberes proteger la información de sus contribuyentes.

- **Enfoque y descripción de la entidad.**

La Secretaría de Educación de Yumbo, es una entidad perteneciente al sector Gobierno de Colombia, cuya misión consiste en la prestación del servicio público educativo.

- **Misión**

  Liderar en el Municipio de Yumbo la prestación del servicio público educativo, con un modelo eficiente, incluyente y sostenible apoyado en la ciencia, la tecnología, la innovación y el emprendimiento para el logro de una educación pertinente y de calidad, que prioriza la

formación del ser humano para la convivencia acorde a las necesidades e intereses de la comunidad, en el contexto sociocultural, económico, ambiental y las exigencias del mundo actual.

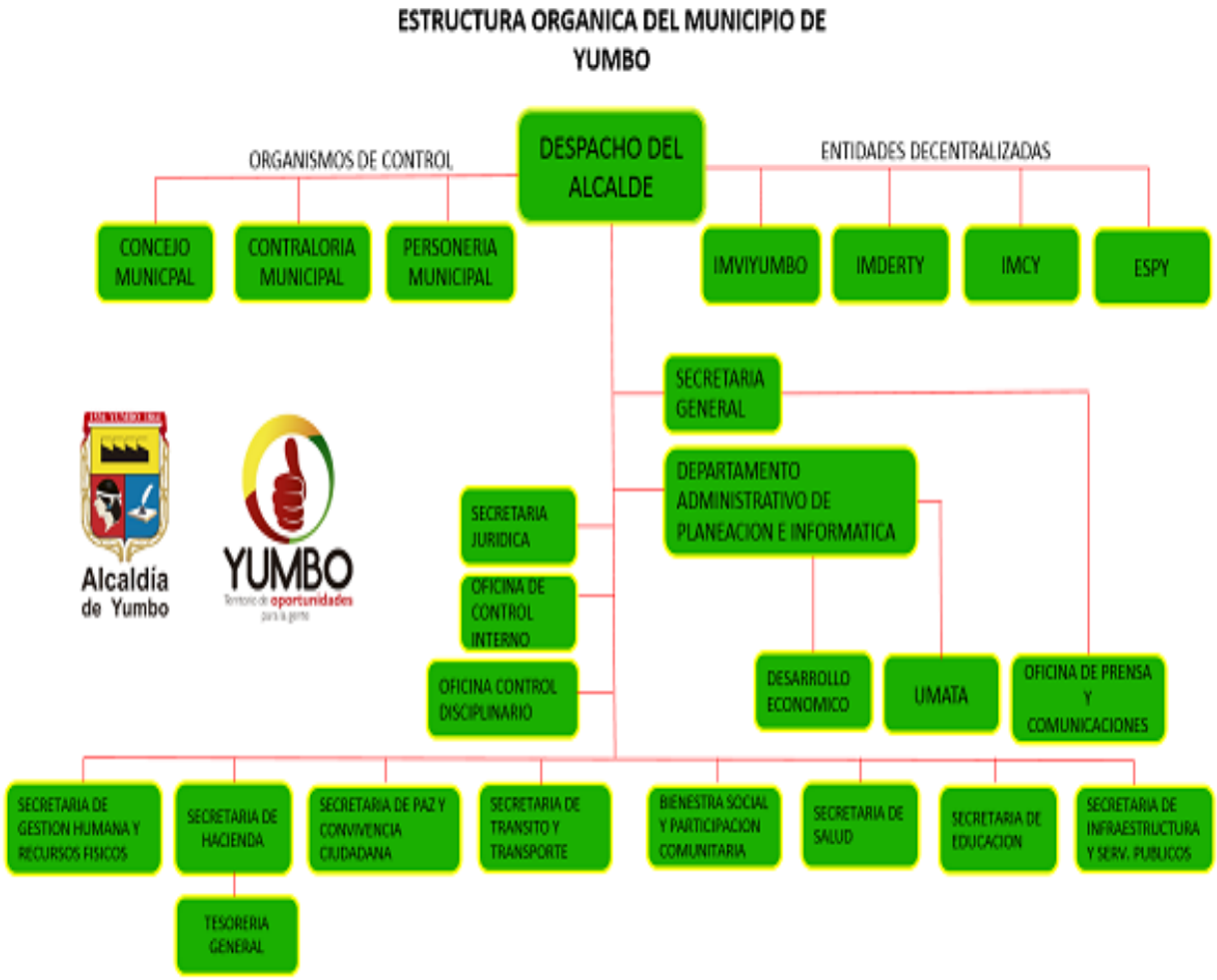
- **Visión**

  En el 2025 la Secretaría de Educación del Municipio de Yumbo brindará el servicio público educativo con un modelo eficiente, incluyente y sostenible apoyado en la ciencia, la tecnología, la innovación y el emprendimiento, para el logro de una educación pertinente y de calidad en todos los niveles desde la primera infancia, la educación básica y media, la educación para el trabajo y la educación superior, garantizando la participación de la comunidad educativa y la dignificación de la labor docente.

5.2.1.2 Organigrama

A continuación, se presenta la estructura Orgánica tanto del Municipio de Yumbo como también la de la Secretaría de Educación Municipal:

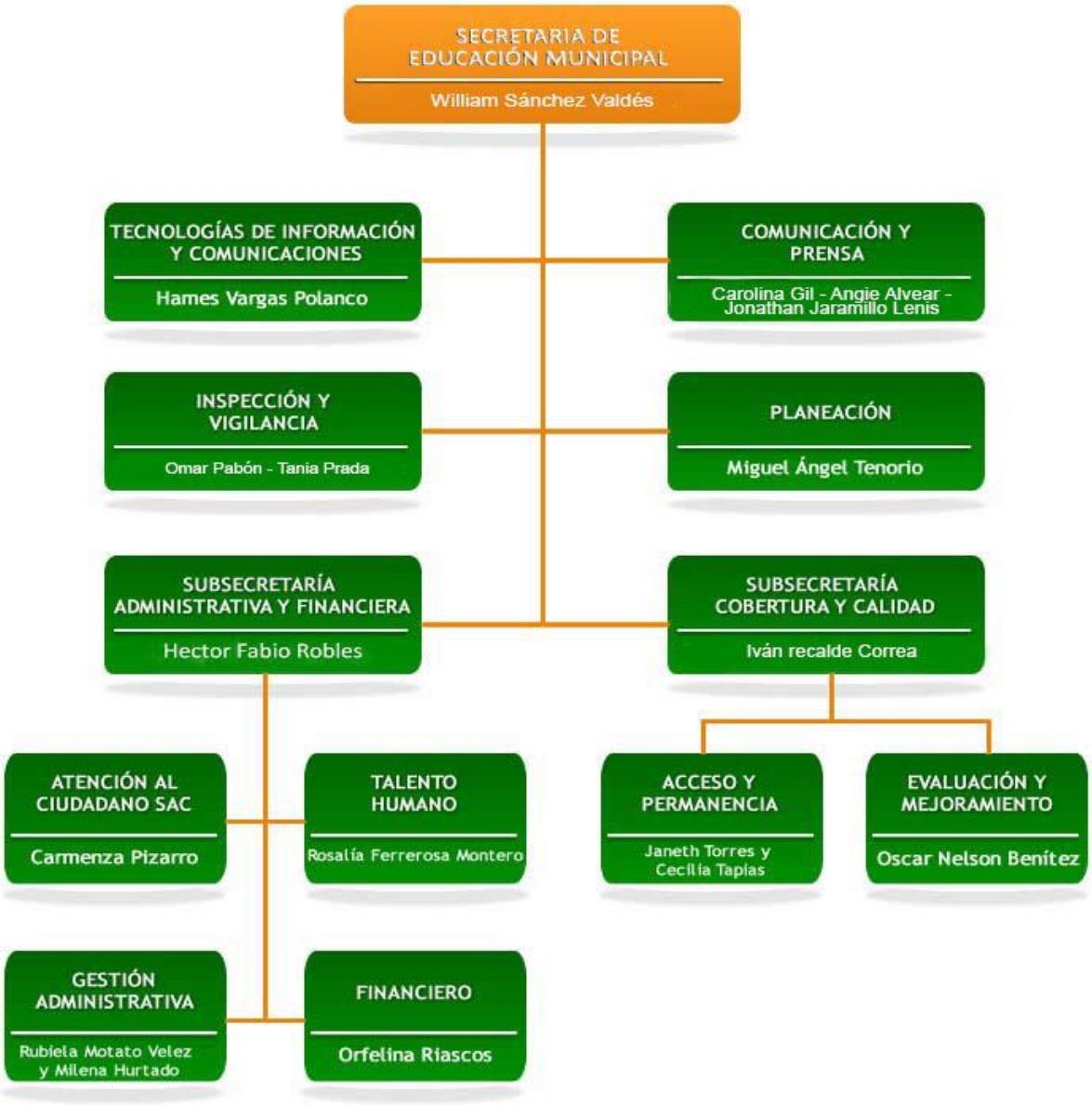
Figura 10. Organigrama Municipio de Yumbo



Fuente: Municipio de Yumbo, (2018, p1).

La anterior figura nos ilustra sobre la estructura organizacional y gerarquica del Municipio de Yumbo.

Figura 11. Organigrama Secretaría de Educación Yumbo



Fuente: Secretaría de Educación Yumbo, (2018,p.1)

La anterior figura nos ilustra sobre la estructura organizacional y gerarquica de la secretaría de educación del Municipio de Yumbo.

5.2.1.3 Funciones de los cargos principales

Tabla 5. Funciones secretario de educación Yumbo

Funciones secretario de educación Yumbo	
I. IDENTIFICACION DEL EMPLEO	
Nivel:	DIRECTIVO
Denominación del Empleo	SECRETARIO DE DESPACHO
Código	020
Grado:	02
Número de cargos:	UNO (1)
Dependencia:	SECRETARIA EDUCACION
Cargo del jefe inmediato:	ALCALDE
II. AREA FUNCIONAL	
Secretaría de educación Municipal Certificada	
III. PROPOSITO PRINCIPAL	
Dirigir, controlar y evaluar el proceso de formulación y ejecución de políticas, estrategias, planes y programas orientados a garantizar la prestación del servicio educativo, la calidad educativa, la ampliación de cobertura, el acceso y permanencia en los diferentes niveles de educación del Municipio de Yumbo, con criterios de eficacia y eficiencia, teniendo en cuenta la normatividad legal vigente.	
• Coordinar el direccionamiento estratégico de las funciones de la secretaria de educación para adoptar los planes, programas y proyectos que garanticen el desarrollo de la política educativa con la eficiente administración de los recursos disponibles y asignados para la jurisdicción. • Dirigir, controlar y evaluar las estrategias para el acceso, permanencia y ampliación de cobertura de la educación en el Municipio de Yumbo de conformidad con las normas vigentes, promoviendo el servicio de educación formal, educación para el trabajo y el desarrollo humano y educación informal en los términos de la Constitución y la Ley.	

Funciones secretario de educación Yumbo

- Dirigir, controlar y evaluar el proceso de calidad educativa para garantizar el mejoramiento continuo de los establecimientos educativos, con base en la gestión integral del capital humano docente, directivo docente y administrativo y de gestión de los recursos pedagógicos, físicos, técnicos, tecnológicos, financieros y demás componentes del sistema de gestión educativa del Municipio de Yumbo.
- Planear, dirigir, controlar y evaluar el proceso de inspección, vigilancia y control de la educación en el Municipio de Yumbo de conformidad con las normas vigentes.
- Dirigir, controlar y evaluar el proceso de gestión administrativas y financiera de la educación oficial en el Municipio de Yumbo de conformidad con las normas vigentes.
- Dirigir, controlar y evaluar los procesos de apoyo de la secretaría de educación tendientes a garantizar el cumplimiento de los lineamientos institucionales y la prestación efectiva del servicio educativo en el Municipio de Yumbo.
- Liderar la interacción y la comunicación permanente con los diferentes grupos de interés y con los actores principales del sistema educativo, orientado a establecer alianzas estratégicas gubernamentales y no gubernamentales, para el mejoramiento continuo del servicio educativo del Municipio de Yumbo.
- Coordinar con las diferentes dependencias de la Administración Central y del sector público de Yumbo, la gestión institucional para garantizar el normal funcionamiento del servicio educativo del Municipio de Yumbo, según necesidades del mismo.
- Coordinar y controlar los procesos de interventoría y supervisión de los contratos que se ejecuten en la dependencia a su cargo, de conformidad con la normatividad vigente.
- Presentar los informes cualitativos y cuantitativos de gestión de la dependencia, técnicos, administrativos y/o financieros, requeridos por los organismos de control, las autoridades, las entidades territoriales o sectoriales, las comunidades y el Alcalde Municipal, en forma oportuna.

Funciones secretario de educación Yumbo

V. CONOCIMIENTOS BASICOS ESENCIALES

- Ley General de Educación.
- Administración del sistema de información del sector educativo.
- Políticas Públicas de educación.
- Administración de los recursos del sector educativo.
- Sistema de evaluación de la calidad de la educación.
- Normatividad de Contratación y presupuesto público.
- Conocimiento e interpretación de indicadores sociales
- Informática básica.

VI. COMPENTENCIAS COMPORTAMENTALES

COMUNES	POR NIVEL JERARQUICO
• Orientación a resultados • Orientación al usuario y al ciudadano • Transparencia • Compromiso con la organización	• Liderazgo • Planeación • Toma de decisiones • Dirección y Desarrollo de Personal • Conocimiento del entorno

VII. REQUISITOS DE FORMACION ACADEMICA Y EXPERIENCIA

FORMACION ACADEMICA	EXPERIENCIA
• Título Profesional en Educación o Administración o Comunicación Social, Periodismo y Afines o Ingeniería de Sistemas, Telemática y Afines o Derecho y Afines. • Tarjeta profesional si aplica. • Título de postgrado en la modalidad de	Treinta y seis (36) meses de experiencia profesional relacionada.

Funciones secretario de educación Yumbo

especialización en áreas de la educación o Derecho Administrativo o relacionadas con las funciones del cargo.	
ALTERNATIVA	
• Título Profesional en Educación o Administración o Comunicación Social, Periodismo y Afines o Ingeniería de Sistemas, Telemática y Afines o Derecho y Afines. • Tarjeta profesional si aplica.	Sesenta (60) meses de experiencia profesional relacionada.

Fuente: Elaborado bajo la referencia de la Secretaría de educación de Yumbo (2018)

A continuación, se relacionan las funciones del subsecretario de Calidad y Cobertura del Municipio de Yumbo:

Tabla 6. Funciones del subsecretario de Calidad y cobertura

Funciones del subsecretario de Calidad y cobertura

I. IDENTIFICACION DEL EMPLEO	
Nivel	DIRECTIVO
Denominación Empleo	SUBSECRETARIO DE DESPACHO
Código	045
Grado	01
Número de cargos	UNO (1)
Dependencia	SECRETARIA DE EDUCACION
Cargo jefe inmediato:	SECRETARIO DE EDUCACION
II. AREA FUNCIONAL	
Sub secretaría de calidad y cobertura de la Secretaria de Educación del municipio de Yumbo- SEMY.	

Funciones del subsecretario de Calidad y cobertura

III. PROPOSITO PRINCIPAL

Mejorar las condiciones de calidad, acceso, permanencia y ampliación de cobertura del servicio educativo del Municipio de Yumbo y cada uno de sus actores, obteniendo como resultado una educación de alto nivel, de reconocimiento regional, reflejada en las pruebas de estado y en la formación de ciudadanos y ciudadanas competitivas, hábiles, investigadores, artistas y pensadores.

IV. DESCRIPCION DE LAS FUNCIONES ESENCIALES

- Coordinar el proceso de apropiación de los lineamientos y metodologías para la incorporación de competencias básicas; evaluación de desempeño de docentes y directivos docentes; autoevaluación institucional y actualización del perfil educativo; construcción o modificación de los proyectos educativos Institucionales- PEI y los Planes de Mejoramiento Institucional- PMI, según disposiciones del Ministerio de Educación Nacional.
- Planear y coordinar las actividades de asistencia técnica a los establecimientos educativos para mejorar falencias detectadas en los insumos administrativos de evaluación integral de la educación en Yumbo y participar en la formulación del Plan de Asistencia Técnica Coordinado de la Secretaria de Educación del municipio de Yumbo- SEMY.
- Elaborar y actualizar el Perfil Educativo y la caracterización del sector educativo del municipio de Yumbo, acorde con los lineamientos del MEN.
- Coordinar, controlar y evaluar el proceso de actualización y ejecución del Plan Territorial de Formación Docente -PTFD- del Municipio de Yumbo.
- Liderar la formulación del Plan de Apoyo al Mejoramiento- PAM, para garantizar el mejoramiento continuo de los establecimientos educativos oficiales del municipio de Yumbo.
- Coordinar la ejecución del direccionamiento estratégico para la prestación del servicio educativo en el Municipio de Yumbo, que garantice el cumplimiento de los componentes y lineamientos contemplados en el proyecto de modernización de las secretarias de educación de los entes territoriales certificados,

Funciones del subsecretario de Calidad y cobertura

emanado por el Ministerio de Educación Nacional- MEN y en concordancia con el marco legal educativo vigente.

- Coordinar, controlar y evaluar el proceso de ejecución del Plan Educativo Municipal de Yumbo y sus correlativos planes de acción anuales.
- Fomentar la investigación, innovación y desarrollo de currículos, métodos y medios pedagógicos que permitan mejorar la efectividad de la educación en Yumbo.
- Recolectar, procesar, analizar y reportar la información del sector educativo del área de calidad y cobertura en la ejecución y seguimiento en el Plan Municipal de Desarrollo de Yumbo.
- Presentar los informes cualitativos y cuantitativos de gestión de la dependencia, técnicos, administrativos y/o financieros, requeridos por los organismos de control, las autoridades, las entidades territoriales o sectoriales, las comunidades y el Alcalde Municipal, en forma oportuna.

V. CONOCIMIENTOS BASICOS ESENCIALES

- Normatividad sobre Políticas Públicas, Institucionales y Sociales en educación
- Sistema de evaluación de la calidad de la educación.
- Metodología plan de desarrollo y plan indicativo
- Metodologías de investigación, diseño y ejecución de proyectos
- Conocimiento e interpretación de indicadores sociales
- Informática básica.

VI. COMPENTENCIAS COMPORTAMENTALES

COMUNES	POR NIVEL JERARQUICO
• Orientación a resultados	• Liderazgo
• Orientación al usuario y al ciudadano	• Planeación
• Transparencia	• Toma de decisiones

Funciones del subsecretario de Calidad y cobertura	
• Compromiso con la organización	• Dirección y Desarrollo de Personal • Conocimiento del entorno
VII. REQUISITOS DE FORMACION ACADEMICA Y EXPERIENCIA	
FORMACION ACADÉMICA	EXPERIENCIA
• Título Profesional en Educación o Administración o Ingeniería de Sistemas, Telemática y Afines. • Tarjeta profesional si aplica. • Título de postgrado en la modalidad de especialización en áreas de la educación o relacionadas con las funciones del cargo.	Veinticuatro (24) meses de experiencia profesional relacionada.
• ALTERNATIVA	
• FORMACION ACADÉMICA	EXPERIENCIA
• Título Profesional en Educación o Administración o Ingeniería de Sistemas, Telemática y Afines. • Tarjeta profesional si aplica.	Cuarenta y ocho (48) meses de experiencia profesional relacionada.

Fuente: Elaborado bajo la referencia de la Secretaría de educación de Yumbo (2018)

A continuación, se relacionan las funciones del Líder TIC de la Secretaría de Educación de Yumbo:

Tabla 7. Funciones Líder TIC Secretaría de Educación

Funciones Líder TIC Secretaría de Educación

I. IDENTIFICACION DEL EMPLEO	
Nivel	PROFESIONAL
Denominación Empleo	PROFESIONAL ESPECIALIZADO
Código	222
Grado	04
Número de cargos	UNO (1)
Dependencia	SECRETARIA DE EDUCACION
Cargo jefe inmediato	SECRETARIO DE EDUCACION

II. AREA FUNCIONAL

Tecnologías de la informática y las comunicaciones en sector educativo de Yumbo

III. PROPOSITO PRINCIPAL

Incorporar el uso de las TIC como eje transversal para fortalecer los procesos de enseñanza y aprendizaje en todos los niveles educativos del Municipio de Yumbo.

IV. DESCRIPCION DE LAS FUNCIONES ESENCIALES

- Realizar estudios de campo, gestionar y entregar información pertinente y oportuna para la implantación de infraestructura: hardware, software, conectividad, en los establecimientos educativos de Yumbo.
- Ser el interlocutor formal de la Secretaría de Educación ante el Ministerio de Educación, específicamente de la Oficina de Innovación Educativa con uso de TIC, en los temas referidos al uso educativo y apropiación pedagógica de TIC en los establecimientos educativos del Municipio Yumbo.
- Liderar procesos de dotación de aulas con computadores educativos en las Instituciones educativas del Municipio de Yumbo.
- Mantener comunicación con los rectores y demás integrantes de la comunidad educativa que se

relacionen con el proyecto de usos de nuevas tecnologías en el sector educativo de Yumbo.

- Consolidar, organizar, estructurar y suministrar información oportuna que permita realizar los estudios de evaluación de impacto y estados del arte sobre los usos y apropiación educativa de TIC en el Municipio de Yumbo.
- Liderar, coordinar y monitorear los diferentes programas de formación de docentes en el uso de TIC, proyectos de innovación educativa y demás estrategias adelantados por el Ministerio de Educación Nacional, por la Secretaría de Educación del Valle, otros entes territoriales y aliados estratégicos de la Secretaría de Educación de Yumbo.
- Fomentar la participación de los docentes, directivos docentes y estudiantes de las Instituciones Educativas en las redes de aprendizaje dispuestas para ellos, por la Secretaría de Educación del Municipio de Yumbo.
- Participar en la toma de decisiones en temas de la incorporación de TIC en los procesos pedagógicos y de gestión de los establecimientos educativos bajo la dirección de la Secretaría de Educación del Municipio de Yumbo.
- Articular los proyectos relacionados con los ejes estratégicos (gestión para el fomento al uso educativo de TIC, formación de docentes en TIC, gestión de contenidos educativos y procesos de gestión de uso y apropiación pedagógica de TIC, acompañamiento a sus establecimientos educativos, infraestructura.) en ejecución en el Municipio de Yumbo.
- Rendir los informes que le sean solicitados con la oportunidad y periodicidad requeridos.

V. CONOCIMIENTOS BASICOS O ESENCIALES

- Renovación pedagógica y uso de TIC en la educación.
- Políticas públicas de innovación educativa en Colombia.
- Sistema Nacional de Innovación.
- Ley de Ciencia y tecnología.

Funciones Líder TIC Secretaría de Educación	
• Plan decenal de educación. • La educación que queremos para la generación de los bicentenarios. • Modelo Estándar de control interno. • Metodologías sobre investigación y formulación de proyectos	
VI. COMPENTENCIAS COMPORTAMENTALES	
COMUNES	POR NIVEL JERARQUICO
• Orientación a resultados • Orientación al usuario y al ciudadano • Transparencia • Compromiso con la organización	• Aprendizaje Continuo • Experticia Profesional • Trabajo en Equipo y Colaboración • Creatividad e Innovación • Liderazgo de Grupos de Trabajo • Toma de decisiones
VII. REQUISITOS DE FORMACION ACADEMICA Y EXPERIENCIA	
FORMACION ACADEMICA	EXPERIENCIA
• Título Profesional en Ingeniería de Sistemas, Telemática y Afines. • Tarjeta profesional. • Título de postgrado en la modalidad de especialización en disciplinas afines con las funciones del cargo.	Treinta y seis (36) meses de experiencia profesional relacionada.

Fuente: Elaborado bajo la referencia de la Secretaría de educación de Yumbo (2018)

La responsabilidad en la seguridad de la información está bajo la responsabilidad de todos los funcionarios de la secretaria de educación.

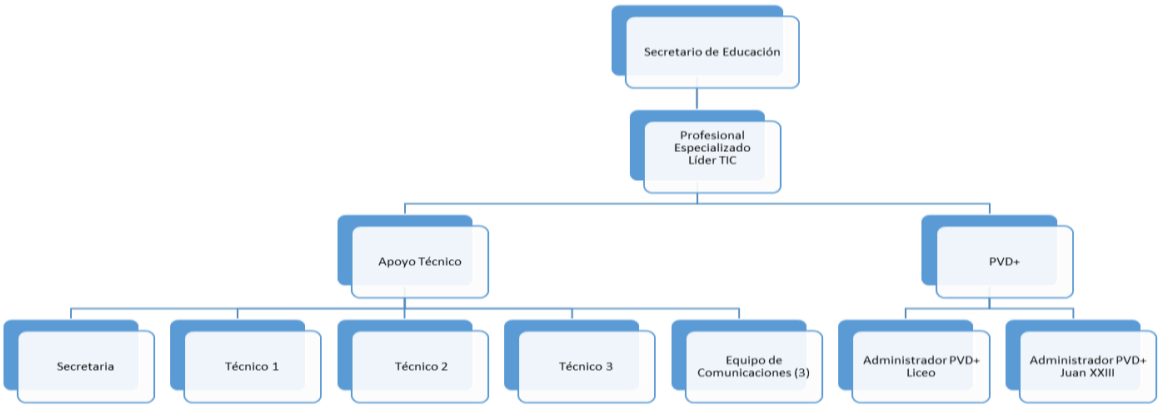
La secretaría de educación cuenta con un grupo de Tecnología de Información y Comunicaciones, liderado por el Ing. Hames Vargas Polanco quien tiene como profesión Ingeniero de sistemas, con especialización en gerencia estratégica de sistemas y especialización en telemática, también cuenta con una Maestría en Ingeniería de sistemas y actualmente cursa último semestre de Maestría en gestión de TI en la Universidad UNAD. El grupo humano TIC está conformado por las siguientes personas:

Tabla 8. Personal TIC Secretaría de educación Yumbo

MUNICIPIO DE YUMBO	
SECRETARIA DE EDUCACIÓN	
CARGOS PERSONAL TIC SECRETARIA DE EDUCACIÓN	
CARGO	**CANTIDAD**
Profesional especializado - Líder TIC	1
Secretaria	1
Técnicos de soporte	3
Equipo de comunicaciones	2
Administradores PVD+	2

Fuente: Elaborado bajo la referencia de la Secretaría de Yumbo (2018)

Figura 12. Organigrama grupo TIC SEM Yumbo



Fuente: Elaborado bajo la referencia de la Secretaría de Yumbo (2018)

5.2.1.4. Políticas, objetivos y las estrategias implementadas para lograrlos

El Municipio de Yumbo no cuenta con ninguna política, normas y buenas prácticas de seguridad de la información que puedan ofrecer confianza a sus ciudadanos. Las situaciones que se presentan al interior de la organización como conflictos o inconformidades de la ciudadanía son atendidas por los diferentes funcionarios, quienes basados en su experiencia se encargan directamente de gestionarlos.

Para el cumplimiento de la Implementación del SGSI, se cuenta con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno en línea de Colombia, Disponible en (MinTIC, 2016), el cuan es el referente utilizado para el presente proyecto de Maestría.

El Líder TIC del Municipio de Yumbo es consciente de la falta de una adecuada gestión de la seguridad, por lo anterior ve la importancia de implantar un Sistema de Gestión de la Seguridad de la información para ser más competitivos y cumplir con lo establecido por el Gobierno Nacional en esta materia.

5.2.2 Criterios básicos.

Teniendo en cuenta el alcance y los objetivos para la Gestión del Riesgo, se detallan los criterios de Evaluación del Riesgo, de impacto y de aceptación del riesgo propuestos:

5.2.2.1 Criterios de evaluación

Para valorar el nivel de seguridad actual de la Empresa se realiza la evaluación utilizando el modelo establecido por la norma ISO 27001 en su anexo A, basado en los niveles de madurez, que consiste en una puntuación de 0 a 100, donde el menor cumplimiento es (0): "Inexistente" y el mayor cumplimiento es (100): "Optimizado".

5.2.2.2 Análisis Gap para la norma ISO/iec27002:2013

Para el diagnóstico de la situación actual del Municipio de Yumbo en materia de seguridad y privacidad de la información, se diligenció el instrumento de evaluación suministrado por el Ministerio de TIC de Colombia, lo cual se ilustró en las figuras 8 y 9 del presente documento, en donde se muestran los resultados del análisis con respecto a los diferentes dominios establecidos en la norma.

- Anexo 1- ISO 27001:2013

De acuerdo con la situación actual se puede observar que la Empresa es consciente de su realidad y ha comenzado a establecer procedimientos para fortalecer los controles para mitigar los riesgos asociados a la seguridad lógica y física.

De la evaluación de los controles, el nivel de madurez indica que la mayor cantidad se encuentran en un estado de “Inexistente” e “Inicial” lo que define principalmente que:

- No se cuenta con un enfoque de administración de seguridad de la información y los pocos aspectos que se han iniciado se encuentran desorganizados.
- Ningún procedimiento asociado a la seguridad han sido documentado
- Existe un alto grado de confianza en el conocimiento del personal
- No hay comunicación formal de los eventos de seguridad, entre otros.

5.2.3 Identificación y Análisis del riesgo

Los activos de información son de suma importancia para toda organización, debido a esto se requiere conocer los recursos de información con los que cuenta la organización, para de esta misma forma iniciar con la implementación del Plan de SGSI.

Como metodología de análisis y gestión de riesgos de la información se utilizó Magerit, la cual fue desarrollada por el Consejo Superior de Administración Electrónica. En esta metodología sobresalen dos objetivos principales, uno de los cuales es estudiar los riesgos que soporta un sistema de información y el entorno asociado a este, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio, y otro relacionado con recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir impedir, reducir o controlar los riesgos investigados.

Magerit clasifica los activos en varios tipos de acuerdo a la función que ejercen en el tratamiento de la información. Como primer paso para el Análisis de riesgos se accedió al inventario de Activos y una clasificación de acuerdo al Tipo.

5.2.3.1 Identificación de los activos

Los activos se agruparán según sus características, valor y criticidad similares acordes con lo establecido en la guía No.7 Guía de gestión de Riegos de MinTIC.

Tabla 9. Grupo de activos

GRUPO	ABREVIATURA	DESCRIPCIÓN
Instalaciones	[L]	Lugares donde se alojan los sistemas de información y comunicaciones.
Hardware	[HW]	Recursos materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
Aplicación	[SW]	Soporte lógico que permite gestionar, analizar y transformar los datos permitiendo la explotación de la información para la prestación de los servicios
Datos:	[D]	El activo que permite a la organización prestar sus Servicios.
Redes de Comunicación	[COM]	Instalaciones dedicadas como servicios de comunicaciones para medios de transporte que llevan datos de un sitio a otro.
Servicios	[S]	Funciones que satisfacen las necesidad de los Usuarios prestados por el sistema.
Equipamiento auxiliar	[AUX]	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
Personal	[P]	Las personas relacionadas con los sistemas de Información.

Fuente: Gobierno de España, (2012, p.8).

- **Tipos de activos**

A continuación, se relacionan los tipos de activos, teniendo en cuenta lo establecido por la metodología Magerit:

AMENAZAS

Lista de catálogo de amenazas posibles sobre los activos de un sistema de información:

[N] Desastres naturales

[N.1] Fuego

[N.2] Daños por agua

[N.*] Desastres naturales

[I] De origen industrial

[I.1] Fuego

[I.2] Daños por agua

[I.*] Desastres industriales

[I.3] Contaminación mecánica

[I.4] Contaminación electromagnética

[I.5] Avería de origen físico o lógico

[I.6] Corte del suministro eléctrico

[I.7] Condiciones inadecuadas de temperatura o humedad

[I.8] Fallo de servicios de comunicaciones

[I.9] Interrupción de otros servicios y suministros esenciales

[I.10] Degradación de los soportes de almacenamiento de la información

[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios

[E.2] Errores del administrador

[E.3] Errores de monitorización (log)

[E.4] Errores de configuración

[E.7] Deficiencias en la organización

[E.8] Difusión de software dañino

[E.9] Errores de [re-]encaminamiento

[E.10] Errores de secuencia

[E.14] Escapes de información

[E.15] Alteración accidental de la información

[E.18] Destrucción de información

[E.19] Fugas de información

[E.20] Vulnerabilidades de los programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)

[E.24] Caída del sistema por agotamiento de recursos

[E.25] Pérdida de equipos

[E.28] Indisponibilidad del personal

[A] Ataques intencionados

[A.3] Manipulación de los registros de actividad (log)

[A.4] Manipulación de la configuración

[A.5] Suplantación de la identidad del usuario

[A.6] Abuso de privilegios de acceso

[A.7] Uso no previsto

[A.8] Difusión de software dañino

[A.9] Reencaminamiento de mensajes

[A.10] Alteración de secuencia

[A.11] Acceso no autorizado

[A.12] Análisis de tráfico

[A.13] Repudio

[A.14] Interceptación de información (escucha)

[A.15] Modificación deliberada de la información

[A.18] Destrucción de información

[A.19] Divulgación de información

[A.22] Manipulación de programas

[A.23] Manipulación de los equipos

[A.24] Denegación de servicio

[A.25] Robo

[A.26] Ataque destructivo

[A.27] Ocupación enemiga

[A.28] Indisponibilidad del personal

[A.29] Extorsión

[A.30] Ingeniería social (picaresca)

Continuando con la metodología, en la siguiente tabla se presentan los activos de información más importantes que actualmente posee el Municipio de Yumbo.

En la siguiente tabla se presentan los activos de información más importantes que actualmente posee el Municipio de Yumbo. Se aclara que la información digital que genera la Secretaría de Educación se Almacena en servidores ubicados en el Departamento

Administrativo de Planeación e Informática del Municipio de Yumbo y en Servidores del Ministerio de Educación Nacional.

Tabla 10. Activos de Información

ÁMBITO	ID	ACTIVO	DESCRIPCIÓN
Instalaciones [L]	[L-01]	Oficina de Sistemas Municipio de Yumbo	Lugares donde se alojan los sistemas de información y comunicaciones Datacenters 1 y 2.
Equipos [HW]	[HW-01]	Servidor Principal - Sistemas	Recursos materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
	[HW-02]	Servidor de Intranet - Sistemas	
	[HW-03 al 36]	Desktop No. 1 al Desktop No.	
Hardware [HW]	[HW-37]	Portátil	
Aplicación [SW]	[SW-01]	Windows 7 Profesional	Soporte lógico que permite gestionar, analizar y transformar los datos permitiendo la explotación de la información para la prestación de los servicios
	[SW-02]	Windows 8 Profesional	
	[SW-03]	Windows 8.1 Profesional	
	[SW-04]	Windows 10 Profesional	
	[SW-05]	Microsoft Office 2007	
	[SW-06]	Microsoft Office 2010	
	[SW-07]	Microsoft Office 2013	
	[SW-08]	Microsoft Office 2016	
	[SW-09]	Antivirus	
	[SW-10]	Windows Server 2008 R2	
	[SW-11]	Linux	
	[SW-12]	Aplicación **Help desk** Vs 0.90.3	
	[SW-13]	Aplicación **Orfeo** 3.8.2	
	[SW-14]	Aplicación **SRFPlus** Vs 3.0.62	
	[SW-15]	Aplicación Gestión de Matrícula	
	[SW-16]	Aplicación Gestión de Recursos	
	[SW-17]	Aplicación Gestión y Control	
	[D-01]	Datos de Empleados, Docentes, Estudiantes, Rectores, Personal	El activo que permite a la organización prestar

ÁMBITO	ID	ACTIVO	DESCRIPCIÓN
Datos[D]	[D-02]	Datos de gestión Administrativa, Contable y Financiera.	sus servicios.
	[D-03]	Datos de soporte técnico	
	[D-04]	Copias de Seguridad	
	[D-05]	Logs	
Red de Comunicación [COM]	[COM-01]	UTM Fortinet	Instalaciones dedicadas como servicios de comunicaciones para medios de transporte que llevan datos de un sitio a otro.
	[COM-02]	Rourter	
	[COM-03]	Access Point	
	[COM-04]	Red Cableada	
	[COM-05]	Red inalámbrica	
Servicios [S]	[S-01]	Correo Electrónico	Funciones que satisfacen las necesidades de los usuarios prestados por el sistema.
	[S-02]	Servicio Web	
Equipamiento auxiliar [AUX]	[AUX-01]	Impresoras	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
	[AUX-02]	UPS	
	[AUX-03]	Aire Acondicionado	
	[AUX-04]	Planta eléctrica	
	[AUX-05]	Archivadores	
Personal [P]	[P-01]	Líder de TI Alcaldía	Las personas relacionadas con los sistemas de información.
	[P-02]	Líder de TI SEMI	
	[P-03]	Demás personal de TI	
	[P-04]	Empleados SEMY	
	[P-05]	Comunidad	

Fuente: Elaboración Propia

No se relacionan más detalles del mismo, atendiendo la Ley 1581 de 2012 de protección de datos de Colombia.

5.2.3.2 Dimensiones de Valoración

La valoración de Activos se realizó teniendo en cuenta las dimensiones de: confiabilidad, integridad, autenticidad, disponibilidad y trazabilidad definidas en Magerit como:

- **Confiabilidad (C)**: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad (I)**: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **Autenticidad (A)**: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Disponibilidad (D)**: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren
- **Trazabilidad (T)**: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

A través de ellas se mostrará el impacto que las diferentes amenazas podrían causar a cada activo. En la siguiente figura se muestran los rangos de valoración:

Figura13. Rangos de Valoración del Riesgo

Rango	valor		criterio
9 -10	muy alto	MA	daño muy grave
6-8	alto	A	daño grave
3-5	medio	M	daño importante
1-2	bajo	B	daño menor
0	Muy Bajo	MB	irrelevante a efectos prácticos

Fuente: disponible en (Gobierno de España, 2012)

5.2.3.3 Valoración del riesgo

Para determinar la calificación cualitativa que nos informa la importancia de los activos, se utiliza la siguiente figura:

Figura 14. Importancia de los activos

valor	criterio	Rango
MA	muy alto	41-50
A	alto	26-40
M	medio	15-25
B	bajo	6-14
MB	Muy Bajo	0-5

Fuente: Gobierno de España, (2012, p.8).

A continuación, se realiza la valoración cuantitativa Valoración de los activos:

Tabla 11. Valoración de los Activos

AMBITO	ID	ACTIVO	ASPECTOS CRITICOS						IMPOR
			[A]	[C]	[I]	[D]	[T]	TOTAL	TANCIA
Instalaciones [L]	[L-01]	Oficina de Sistemas Municipio deYumbo	8	10	8	10	5	41	MA
	[HW-01]	Servidor Principal - Sistemas	8	10	10	10	10	48	MA
	[HW-02]	Servidor de Intranet - Sistemas	7	8	8	9	5	37	A
	[HW-03 al 36]	Desktop No. 1 al Desktop No. 34	3	2	1	1	1	8	B

AMBITO	ID	ACTIVO	ASPECTOS CRITICOS						IMPOR
			[A]	[C]	[I]	[D]	[T]	TOTAL	TANCIA
Hardware [HW]	[HW-37]	Portátil	3	2	1	1	1	8	B
	[SW-01]	Windows 7 Profesional	5	2	5	5	3	20	M
	[SW-02]	Windows 8 Profesional	5	2	5	5	3	20	M
	[SW-03]	Windows 8.1 Profesional	5	2	5	5	3	20	M
	[SW-04]	Windows 10 Profesional	5	2	5	5	3	20	M
	[SW-05]	Microsoft Office 2007 Profesional	5	2	5	5	3	20	M
	[SW-06]	Microsoft Office 2010 Profesional	5	2	5	5	3	20	M
	[SW-07]	Microsoft Office 2013 Profesional	5	2	5	5	3	20	M
	[SW-08]	Microsoft Office 2016 Profesional	5	2	5	5	3	20	M
Aplicación [SW]	**[SW-09]**	**Antivirus**	**3**	**8**	**8**	**8**	**6**	**33**	**A**
	[SW-10]	Windows Server 2008 R2	7	9	9	8	8	41	MA
	[SW-11]	Linux	3	8	9	3	7	30	A
	[SW-12]	Aplicación **Help desk** Vs 0.90.3	3	9	3	3	2	20	M
	[SW-13]	Aplicación **Orfeo** 3.8.2	2	8	9	8	7	34	A
	[SW-1]	Aplicación **SRFPlus** Vs 3.0.62 R20070302	2	8	9	8	7	34	A
	[SW-15]	Aplicación Gestión de Matrícula **SIMAT**	2	3	2	1	1	9	B

AMBITO	ID	ACTIVO	ASPECTOS CRITICOS						IMPOR
			[A]	[C]	[I]	[D]	[T]	TOTAL	TANCIA
	[SW-16]	**Aplicación Gestión de Recursos Humanos RRHH**	3	2	1	1	1	8	B
	[SW-17]	Aplicación Gestión y Control Financiero SGCF	2	3	4	1	3	13	B
	[D-01]	Datos de Empleados, Docentes, Estudiantes, Rectores, Personal Administrativo, Padres de familia, Establecimientos Educativos	5	9	9	8	6	37	A
	[D-02]	Datos de gestión Administrativa, Contable y Financiera.	7	8	8	9	5	37	A
	[D-03]	Datos de soporte técnico	3	2	1	2	1	9	B
Datos[D]	[D-04]	Copias de Seguridad	5	9	9	8	6	37	A
	[D-05]	Logs	5	9	9	8	6	37	A
	[COM-01]	UTM Fortinet	5	9	9	8	6	37	A
	[COM-02]	Rourter	4	7	9	7	5	32	A
Red de Comunicación [COM]	**[COM-03]**	**Access Point**	**4**	**7**	**9**	**7**	**5**	**32**	**A**
	[COM-04]	Red Cableada	4	7	9	7	5	32	A
	[COM-05]	Red inalámbrica	4	7	9	7	5	32	A
Servicios [S]	[S-01]	Correo Electrónico	3	6	6	3	5	23	M
	[S-02]	Servicio Web	3	2	3	5	5	18	M
	[AUX-01]	Impresoras	0	0	0	4	0	4	MB
	[AUX-02]	UPS	8	9	9	9	8	43	MA

AMBITO	ID	ACTIVO	ASPECTOS CRITICOS						IMPOR
			[A]	[C]	[I]	[D]	[T]	TOTAL	TANCIA
Equipamiento auxiliar [AUX]		[AUX-03]	Aire Acondicionado	3	2	3	5	5	18	M
		[AUX-04]	Planta eléctrica	3	6	6	3	5	23	M
		[AUX-05]	Archivadores	3	3	5	5	4	20	M
		[P-01]	Líder de TI Alcaldía	5	9	9	8	6	37	A
		[P-02]	Líder de TI SEMI	5	9	9	8	6	37	A
		[P-03]	Demás personal de TI	4	5	3	5	3	20	M
Personal [P]		[P-04]	Empleados SEMY	4	5	3	5	3	20	M
		[P-05]	Comunidad	4	5	3	5	3	20	M

Fuente: Elaboración Propia

Se destaca en esta valoración dada, la importancia muy alta la oficina de sistemas con sus dos Datacenter, el servidor de aplicaciones y de bases de datos, el sistema operativo de servidor y alta la red de comunicaciones entre otras, teniendo en cuenta la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad.

5.2.3.4 Identificación y análisis de amenazas

Los activos se encuentran constantemente expuestos a amenazas de diferentes tipos que pueden reducir su uso y valor. Es necesario identificar dichas amenazas e indicar la frecuencia de ocurrencia, teniendo en cuenta que la materialización de dichas amenazas sobre el activo hará que su valor disminuya porcentualmente.

La siguiente figura muestra la valoración de las amenazas por dimensión:

Figura 15. Formato para Valoración de amenazas

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS [A]	[C]	[I]	[D]	[T]
[N.1]	Fuego	MP	1				100%	
[N.2]	Daños por agua	MP	1				70%	
[I.1]	Fuego	MP	1				100%	
[I.2]	Daños por agua	PF	0,1				50%	
[A.7]	Uso no previsto	N	1				20%	
[A.11]	Acceso no autorizado	PF	0,1		30%	30%		
[A.26]	Ataque destructivo	MP	0,01				100%	
Ámbito: Instalaciones	**Activo: [L-01] Oficina de Sistemas**	N	1,00	0,00	0,30	0,30	1,00	0,00

Fuente: Gobierno de España, (2012. p.8).

La valoración de amenazas es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo en la Secretaria de Educación de Yumbo.

Los diferentes activos de la Secretaria de Educación de Yumbo se encuentran constantemente expuestos a amenazas de diferentes tipos que pueden reducir su uso y valor. Es necesario identificar dichas amenazas e indicar la frecuencia de ocurrencia, teniendo en cuenta que la

materialización de dichas amenazas sobre el activo hará que su valor disminuya porcentualmente.

Se define el tipo de amenazas que puede afectar los activos según su categoría, se toma como referencia la definición de Magerit.

Las siguientes tablas muestra la valoración de amenazas por dimensiones de cada uno de los ámbitos de la Secretaría de Educación de Yumbo que será diligenciada de acuerdo al contexto:

Tabla 12. Matriz para la valoración de amenazas - ámbito: instalaciones

				ASPECTOS CRITICOS				
AMENAZAS:		FRECUENCIA		**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[N.1]	Fuego	MF	0				100%	
[N.2]	Daños por agua	MF	0				100%	
[I.1]	Fuego	MF	0				100%	
[I.2]	Daños por agua	PF	0,1				100%	
[I.3]	Contaminación mecánica	PF	0,1				50%	
[I.5]	Avería de origen físico o lógico	PF	0,1				50%	
[I.6]	Corte del suministro eléctrico	MF	0				50%	
[I.7]	Condiciones inadecuadas de temperatura o humedad	PF	0,1				100%	
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	PF	0,1				100%	
[E.24]	Caída del sistema por agotamiento de recursos	N	1				50%	
[E.25]	Pérdida de equipos	PF	0,1		100%		100%	

				ASPECTOS CRITICOS				
AMENAZAS:		FRECUENCIA		**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[A.6]	Abuso de privilegios de acceso	N	1		100%		100%	
[A.7]	Uso no previsto	N	1		100%	30%	100%	
[A.11]	Acceso no autorizado	PF	0,1		50%	30%		
[A.23]	Manipulación de los equipos	PF	0,1		50%	20%	50%	
[A.24]	Denegación de servicio	F	10				100%	
[A.25]	Robo	MF	0		100%		100%	
[A.26]	Ataque destructivo	MF	0				100%	
	Activo:							
	[HW-01] Servidor Principal - Sistemas							
Ámbito: Hardware	**[HW-02] Servidor de Intranet - Sistemas**	F	10	0	1	0,3	1	0
	[HW-03 al 36]Desktop No. 1 al Desktop No. 34							
	[HW-37] Portátil							

Fuente: Elaboración Propia

Analizando la valoración dada al ámbito de instalaciones, se encuentra que están expuestas actualmente a un alto riesgo de amenazas naturales, industriales y ataques intencionados, lo que implica de manera prioritaria implementar controles o salvaguardas para minimizar los riesgos.

Tabla 13. Matriz para la valoración de Amenazas - ámbito: hardware

				ASPECTOS CRITICOS				
AMENAZAS:		FRECUENCIA		**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[N.1]	Fuego	MF	0				100%	
[N.2]	Daños por agua	MF	0				100%	
[I.1]	Fuego	MF	0				100%	

				ASPECTOS CRITICOS				
AMENAZAS:		FRECUENCIA		**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[I.2]	Daños por agua	PF	0,1				100%	
[I.3]	Contaminación mecánica	PF	0,1				50%	
[I.5]	Avería de origen físico o lógico	PF	0,1				50%	
[I.6]	Corte del suministro eléctrico	MF	0				50%	
[I.7]	Condiciones inadecuadas de temperatura o humedad	PF	0,1				100%	
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	PF	0,1				100%	
[E.24]	Caída del sistema por agotamiento de recursos	N	1				50%	
[E.25]	Pérdida de equipos	PF	0,1		100%		100%	
[A.6]	Abuso de privilegios de acceso	N	1		100%		100%	
[A.7]	Uso no previsto	N	1		100%	30%	100%	
[A.11]	Acceso no autorizado	PF	0,1		50%	30%		
[A.23]	Manipulación de los equipos	PF	0,1		50%	20%	50%	
[A.24]	Denegación de servicio	F	10				100%	
[A.25]	Robo	MF	0		100%		100%	
[A.26]	Ataque destructivo	MF	0				100%	
	Activo:							
	[HW-01] Servidor Principal - Sistemas							
Ámbito: Hardware	**[HW-02] Servidor de Intranet - Sistemas**	F	10	0	1	0,3	1	0

			ASPECTOS CRITICOS				
AMENAZAS:		FRECUENCIA	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
	[HW-03 al 36]Desktop No. 1 al Desktop No. 34						
	[HW-37] Portátil						

Fuente: Elaboración propia

La valoración de Amenazas del ámbito hardware nos muestra la alta probabilidad de amenazas de errores y fallos no intencionados como también de ataques intencionados, lo anterior se evidencia en el literal 5.2.3 del presente documento.

Tabla 14. Matriz para la valoración de amenazas - ámbito: aplicaciones

				ASPECTOS CRITICOS				
AMENAZAS:		FRECUENCIA		**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[E.1]	Errores de los usuarios	N	1		2%	2%	2%	
[E.2]	Errores de Administrador	PF	0,1		30%	20%	20%	
[E.8]	Difusión de software dañino	PF	0,1		5%	5%	5%	
[E.15]	Alteración accidental de la información	MF	100			20%		
[E.18]	Destrucción de información	N	1				30%	
[E.19]	Fugas de información	MF	100		50%			
[E.20]	Vulnerabilidades de los programas (software)	MF	100		50%	20%	5%	
[E.21]	Errores de mantenimiento / actualización de programas (software)	MF	100		1%	2%	2%	
[A.5]	Suplantación de la identidad del usuario	PF	0,1	100%	100%	50%		
[A.6]	Abuso de privilegios de acceso	N	1		50%	20%	20%	
[A.7]	Uso no previsto	N	1		5%	5%	100%	
[A.8]	Difusión de software dañino	PF	0,1		100%	100%	100%	

				ASPECTOS CRITICOS				
AMENAZAS:		FRECUENCIA		**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[A.11]	Acceso no autorizado	PF	0,1		50%	30%		
[A.15]	Modificación deliberada de la información	N	1			50%		
[A.18]	Destrucción de información	PF	0,1				50%	
[A.19]	Divulgación de información	N	1		50%			
[A.22]	Manipulación de programas	PF	0,1		50%	50%	50%	
	Activo:							
Ámbito: Aplicaciones	**[SW-01] Windows 7 Profesional**	MF	100	1	1	1	1	0
	[SW-02] Windows 8 Profesional							
	[SW-03] Windows 8.1 Profesional							
	[SW-04] Windows 10 Profesional							
	[SW-05] Microsoft Office 2007 Profesional							
	[SW-06] Microsoft Office 2010 Profesional							
	[SW-07] Microsoft Office 2013 Profesional							
	[SW-08] Microsoft Office 2016 Profesional							
	[SW-09] Antivirus							
	[SW-10] Windows Server 2008 R2							
	[SW-11] Linux							
	[SW-12] Aplicación Help desk Vs 0.90.3							
	[SW-13] Aplicación Orfeo 3.8.2							
	[SW-14] Aplicación SRFPlus Vs 3.0.62 R20070302							
	[SW-15] Aplicación Gestión de Matrícula							

			ASPECTOS CRITICOS				
AMENAZAS:		FRECUENCIA	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
	SIMAT						
	[SW-16] Aplicación Gestión de Recursos Humanos RRHH						
	[SW-17] Aplicación Gestión y Control Financiero SGCF						

Fuente: Elaboración propia

En el ámbito aplicaciones se encuentra la mayor amenaza en la difusión de software dañino, la falta de políticas de seguridad, de capacitación de los usuarios y de antivirus sin actualización, se convierte en una gran vulnerabilidad a los sistemas de información del Municipio de Yumbo.

Tabla 15. Matriz para la valoración de amenazas - ámbito: datos

AMENAZAS:		**FRECUENCIA**		**ASPECTOS CRITICOS**				
				[A]	**[C]**	**[I]**	**[D]**	**[T]**
[E.1]	Errores de los usuarios	N	1			20%		
[E.2]	Errores de Administrador	PF	0,1		20%	30%	30%	
[E.4]	Errores de configuración (conf)	MF	100			20%	5%	
[E.14]	Escapes de información	F	10		50%			
[E.15]	Alteración accidental de la información	MF	100			30%		
[E.18]	Destrucción de información	N	1				50%	

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[E.19]	Fugas de información	MF	100		30%			
[A.5]	Suplantación de la identidad del usuario	PF	0,1	100%	50%	20%		
[A.6]	Abuso de privilegios de acceso	N	1		30%	5%		
[A.15]	Modificación deliberada de la información	N	1			30%		
[A.18]	Destrucción de información	PF	0,1				100%	
[A.19]	Divulgación de información	N	1		100%			
Ámbito: Datos	**Activo:** **[D-01] Datos de Empleados, Docentes, Estudiantes, Rectores, Personal Administrativo, Padres de familia, Establecimientos Educativos** **[D-02] Datos de gestión Administrativa, Contable y Financiera.** **[D-03] Datos de soporte**	MF	100	100%	100%	30%	100%	0%

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	**[C]**	**[I]**	**[D]**	**[T]**
	técnico							
	[D-04] Copias de Seguridad							
	[D-05] Logs							

Fuente: Elaboración propia

En el ámbito de datos, se valora alto la probabilidad de divulgación de datos sensibles de la comunidad académica del Municipio de Yumbo, generada por la falta de controles y políticas de seguridad.

Tabla 16. Matriz para la valoración de amenazas - ámbito: red de comunicaciones

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[E.2]	Errores de Administrador	PF	0,1		20%	5%	50%	
[E.9]	Errores de reencaminamiento	PF	0,1		5%			
[E.10]	Errores de secuencia	PF	0,1			5%		
[E.14]	Escapes de información	MF	100		5%			
[E.24]	Caída del sistema	N	1				50%	

	por agotamiento de recursos						
[A.5]	Suplantación de la identidad del usuario	PF	0,1	50%	30%		
[A.6]	Abuso de privilegios de acceso	N	1			30%	
[A.7]	Uso no previsto	N	1		5%	5%	50%
[A.9]	Reencaminamiento de mensajes	PF	0,1		5%		
[A.10]	Alteración de secuencia	PF	0,1			5%	
[A.11]	Acceso no autorizado	PF	0,1		50%	30%	
[A.12]	Análisis de tráfico	PF	0,1		30%		
[A.14]	Interceptación de información (escucha)	PF	0,1		50%		
[A.24]	Denegación de servicio	F	10				50%
	Activo:						
	[COM-01] UTM Fortinet						

Ámbito: Red de Comunicación	**[COM-02] Rourter [COM-03] Access Point [COM-04] Red Cableada [COM-05] Red inalámbrica**	MF	100	100%	100%	100%	100%	100%

Fuente: Elaboración propia

En el ámbito: red de comunicaciones se evidencia la mayor amenaza en el cableado de red alámbrica, encontrándose los rack de los datacenter desorganizados y sin una adecuada identificación, lo que dificulta la gestión y administración del mismo, poniendo en peligro la continuidad, seguridad y disponibilidad de la información de la Alcaldía de Yumbo.

Tabla 17. Matriz para la valoración de amenazas - ámbito: servicios

AMENAZAS:		**FRECUENCIA**		**ASPECTOS CRITICOS**				
				[A]	**[C]**	**[I]**	**[D]**	**[T]**
[E.1]	Errores de los usuarios	N	1		5%	2%	2%	
[E.2]	Errores de Administrador	PF	0,1		5%	20%	20%	
[E.15]	Alteración accidental	MF	100			5%		

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
	de la información							
[E.18]	Destrucción de información	N	1				100%	
[E.19]	Fugas de información	MF	100		20%			
[A.5]	Suplantación de la identidad del usuario	PF	0,1	100%	50%	20%		
[A.6]	Abuso de privilegios de acceso	N	1		20%	50%	20%	
[A.7]	Uso no previsto	N	1		5%	5%	50%	
[A.8]	Difusión de software dañino	PF	0,1		50%	50%	50%	
[A.10]	Acceso no autorizado	PF	0,1		30%	30%		
[A.13]	Repudio	PF	0,1					100%
[A.15]	Modificación	N	1			50%		

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
	deliberada de la información							
[A.19]	Divulgación de información	N	1		100%			
[A.24]	Denegación de servicio	F	10				100%	
Ámbito:	**Activo:**							
Servicios	**[S-01] Correo Electrónico**	MF	100	100%	100%	50%	100%	100%
	[S-02] Servicio Web							

Fuente: Elaboración propia

La valoración del ámbito servicios nos muestra como el inadecuado uso del correo electrónico, de la asignación y compartir claves de usuario se convierte en el mayor riesgo de vulnerabilidad a los sistemas de información.

Tabla 18. Matriz para la valoración de amenazas - ámbito: equipamiento auxiliar

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[E.1]	Errores de los usuarios	N	1		5%	2%	2%	

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[E.2]	Errores de Administrador	PF	0,1		5%	20%	20%	
[E.15]	Alteración accidental de la información	MF	100			5%		
[E.18]	Destrucción de información	N	1				100%	
[E.19]	Fugas de información	MF	100		20%			
[A.5]	Suplantación de la identidad del usuario	PF	0,1	100%	50%	20%		
[A.6]	Abuso de privilegios de acceso	N	1		20%	50%	20%	
[A.7]	Uso no previsto	N	1		5%	5%	50%	
[A.8]	Difusión de software dañino	PF	0,1		50%	50%	50%	

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[A.10]	Acceso no autorizado	PF	0,1		30%	30%		
[A.13]	Repudio	PF	0,1					100%
[A.15]	Modificación deliberada de la información	N	1			50%		
[A.19]	Divulgación de información	N	1		100%			
[A.24]	Denegación de servicio	F	10				100%	
Ámbito: Servicios	**Activo:**							
	[S-01] Correo Electrónico	MF	100	100%	100%	50%	100%	100%
	[S-02] Servicio Web							

Fuente: Elaboración propia

El ámbito equipamiento auxiliar nos muestra la probabilidad de amenaza en la posible destrucción de información, repudio y divulgación de la misma. UPS sin condiciones adecuadas de temperatura.

Tabla 19. Matriz para la valoración de amenazas ámbito: personal o recurso humano

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS

				[A]	[C]	[I]	[D]	[T]
[E.7]	Deficiencias y fallos en la organización	F	10				5%	
[E.19]	Fugas de información	MF	100		20%			
[E.28]	Indisponibilidad del personal	N	1				100%	
[A.29]	Extorsión	MP	0		5%	5%	5%	
[A.30]	Ingeniería social	MP	0		5%	5%	5%	
	Activo:							
	[P-01] Líder de TI Alcaldía							
Ámbito: Personal	**[P-02] Líder de TI SEMI** **[P-03] Demás personal de TI** **[P-04] Empleados SEMY** **[P-05] Comunidad**	MF	100	0%	20%	5%	100%	0%

Fuente: Elaboración propia

La posible fuga de información y la indisponibilidad de personal es una amenaza inminente en el ámbito personal o recurso humano, generada por la contratación de mucho personal temporal y la no existencia de cláusulas de confidencialidad en los contratos de vinculación laboral.

Tampoco existen controles adecuados tanto físicos como lógicos al personal.

5.2.3.5 Evaluación del riesgo

- **Impacto potencial.** En la Secretaria de Educación de Yumbo después de haber obtenido los valores de los diferentes activos y la tabla de valoración de amenazas, se determina el impacto potencial que ocasionaría la materialización de dichas amenazas. Se trata de un dato relevante, ya que permitirá priorizar el plan de acción, y a su vez, evaluar cómo se ve modificado

dicho valor una vez se apliquen los controles para mejorar los procesos donde se deben aplicar diferentes metodologías. A continuación, se presenta el impacto potencial en la tabla:

Tabla 20. Impacto potencial

ID	ACTIVO	ASPECTOS CRITICOS					IMPORTANCIA	AMENAZAS					IMPACTO				
		[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[L-01]	Oficina de Sistemas Municipio deYumbo	8	10	8	10	5	MA	0	0,3	0,3	1.0	0	0	3	2,4	1	0
[HW-01]	Servidor Principal - Sistemas	8	10	10	10	10	MA	0	1	0,3	1	0	0	10	3	10	0
[HW-02]	Servidor de Intranet - Sistemas	7	8	8	9	5	A	0	1	0,3	1	0	0	8	2,4	9	0
[HW-03 al 36]	Desktop No. 1 al Desktop No. 34	3	2	1	1	1	B	0	1	0,3	1	0	0	2	0,3	1	0
[HW-37]	Portátil	3	2	1	1	1	B	0	1	0,3	1	0	0	2	0,3	1	0
[SW-01]	Windows 7 Profesional	5	2	5	5	3	M	1	1	1	1	0	5	2	5	5	0
[SW-02]	Windows 8 Profesional	5	2	5	5	3	M	1	1	1	1	0	5	2	5	5	0
[SW-03]	Windows 8.1 Profesional	5	2	5	5	3	M	1	1	1	1	0	5	2	5	5	0

ID	ACTIVO	ASPECTOS CRITICOS					IMPORTANCIA	AMENAZAS					IMPACTO				
		[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[SW-04]	Windows 10 Profesional	5	2	5	5	3	M	1	1	1	1	0	5	2	5	5	0
[SW-05]	Microsoft Office 2007 Profesional	5	2	5	5	3	M	1	1	1	1	0	5	2	5	5	0
[SW-06]	Microsoft Office 2010 Profesional	5	2	5	5	3	M	1	1	1	1	0	5	2	5	5	0
[SW-07]	Microsoft Office 2013 Profesional	5	2	5	5	3	M	1	1	1	1	0	5	2	5	5	0
[SW-08]	Microsoft Office 2016 Profesional	5	2	5	5	3	M	1	1	1	1	0	5	2	5	5	0
[SW-09]	Antivirus	3	8	8	8	6	A	1	1	1	1	0	3	8	8	8	0
[SW-10]	Windows Server 2008 R2	7	9	9	8	8	MA	1	1	1	1	0	7	9	9	8	0
[SW-11]	Linux	3	8	9	3	7	A	1	1	1	1	0	3	8	9	3	0

ID	ACTIVO	ASPECTOS CRITICOS					IMPORTANCIA	AMENAZAS					IMPACTO				
		[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[SW-12]	Aplicación **Help desk** Vs 0.90.3	3	9	3	3	2	M	1	1	1	1	0	3	9	3	3	0
[SW-13]	Aplicación **Orfeo** 3.8.2	2	8	9	8	7	A	1	1	1	1	0	2	8	9	8	0
[SW-14]	Aplicación **SRFPlus** Vs 3.0.62 R20070302	2	8	9	8	7	A	1	1	1	1	0	2	8	9	8	0
[SW-15]	Aplicación Gestión de Matrícula **SIMAT**	2	3	2	1	1	B	1	1	1	1	0	2	3	2	1	0
[SW-16]	Aplicación Gestión de Recursos Humanos **RRHH**	3	2	1	1	1	B	1	1	1	1	0	3	2	1	1	0
[SW-17]	Aplicación Gestión y Control Financiero **SGCF**	2	3	4	1	3	B	1	1	1	1	0	2	3	4	1	0
[D-01]	Datos de Empleados, Docentes, Estudiantes, Rectores, Personal Administrativo, Padres de	5	9	9	8	6	A	100%	100%	30%	100%	0%	5	9	7	8	0

ID	ACTIVO	ASPECTOS CRITICOS					IMPORTANCIA	AMENAZAS					IMPACTO				
		[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[D-02]	Datos de gestión Administrativa, Contable y Financiera.	7	8	8	9	5	A	100%	100%	30%	100%	0%	7	8	2,4	9	0
[D-03]	Datos de soporte técnico	3	2	1	2	1	B	100%	100%	30%	100%	0%	3	2	0,3	2	0
[D-04]	Copias de Seguridad	5	9	9	8	6	A	100%	100%	30%	100%	0%	5	9	2,7	8	0
[D-05]	Logs	5	9	9	8	6	A	100%	100%	30%	100%	0%	5	9	2,7	8	0
[COM-01]	UTM Fortinet	5	9	9	8	6	A	50%	50%	30%	50%	0%	2,5	4,5	2,7	4	0
[COM-02]	Rourter	4	7	9	7	5	A	50%	50%	30%	50%	0%	2	3,5	2,7	3,5	0
[COM-03]	Access Point	4	7	9	7	5	A	50%	50%	30%	50%	0%	2	3,5	2,7	3,5	0
[COM-04]	Red Cableada	4	7	9	7	5	A	100%	100%	100%	50%	100%	2	3,5	2,7	3,5	0

ID	ACTIVO	ASPECTOS CRITICOS					IMPOR TANCIA	AMENAZAS					IMPACTO				
		[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[D-02]	Datos de gestión Administrativa, Contable y Financiera.	7	8	8	9	5	A	100%	100%	30%	100%	0%	7	8	2,4	9	0
[D-03]	Datos de soporte técnico	3	2	1	2	1	B	100%	100%	30%	100%	0%	3	2	0,3	2	0
[D-04]	Copias de Seguridad	5	9	9	8	6	A	100%	100%	30%	100%	0%	5	9	2,7	8	0
[D-05]	Logs	5	9	9	8	6	A	100%	100%	30%	100%	0%	5	9	2,7	8	0
[COM-01]	UTM Fortinet	5	9	9	8	6	A	50%	50%	30%	50%	0%	2,5	4,5	2,7	4	0
[COM-02]	Rourter	4	7	9	7	5	A	50%	50%	30%	50%	0%	2	3,5	2,7	3,5	0
[COM-03]	Access Point	4	7	9	7	5	A	50%	50%	30%	50%	0%	2	3,5	2,7	3,5	0
[COM-04]	Red Cableada	4	7	9	7	5	A	100%	100%	100%	100%	100%	4	7	9	7	5
[COM-05]	Red inalámbrica	4	7	9	7	5	A	50%	50%	30%	50%	0%	2	3,5	2,7	3,5	0
[S-01]	Correo Electrónico	3	6	6	3	5	M	100%	100%	50%	100%	100%	3	6	3	3	5
[S-02]	Servicio Web	3	2	3	5	5	M	100%	100%	50%	100%	100%	3	2	1,5	5	5
[AUX-01]	Impresoras	0	0	0	4	0	MB	0%	5%	5%	100%	0%	0	0	0	4	0
[AUX-02]	UPS	8	9	9	9	8	MA	0%	5%	5%	100%	0%	0	0,45	0,45	9	0
[AUX-03]	Aire Acondicionado	3	2	3	5	5	M	0%	5%	5%	100%	0%	0	0,1	0,15	5	0
[AUX-04]	Planta eléctrica	3	6	6	3	5	M	0%	5%	5%	100%	0%	0	0,3	0,3	3	0
[AUX-05]	Archivadores	3	3	5	5	4	M	0%	5%	5%	100%	0%	0	0,15	0,25	5	0
[P-01]	Líder de TI Alcaldía	5	9	9	8	6	A	0%	20%	5%	100%	0%	0	1,8	0,45	8	0
[P-02]	Líder de TI SEMI	5	9	9	8	6	A	0%	20%	5%	100%	0%	0	1,8	0,45	8	0

ID	ACTIVO	ASPECTOS CRITICOS					IMPOR TANCIA	AMENAZAS					IMPACTO				
		[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[P-03]	Demás personal de TI	4	5	3	5	3	M	0%	20%	5%	100%	0%	0	1	0,15	5	0
[P-04]	Empleados SEMY	4	5	3	5	3	M	0%	20%	5%	100%	0%	0	1	0,15	5	0
[P-05]	Comunidad	4	5	3	5	3	M	0%	20%	5%	100%	0%	0	1	0,15	5	0

Fuente: Elaboración propia

5.2.3.6 Análisis del riesgo

El objetivo de este análisis es asignar números reales y significativos a todos los elementos de este proceso como costos de los controles, el valor de los activos, impacto del negocio, la amenaza de la frecuencia de ocurrencia, la efectividad de los controles, probabilidad de que una amenaza ocurra entre otras cosas en la Secretaria de Educción Yumbo.

Una vez calculado el nivel del Impacto Potencial por cada activo, de igual forma se deberá calcular el nivel del riesgo al cual se encuentra sometida la Secretaria de Educación de Yumbo. De esta manera se podrá definir si se implementan controles o no, estableciendo un nivel de riesgo aceptable, de tal manera que se puedan designar recursos para implementar controles que ayuden a minimizar los riegos sobre los activos que superen los niveles de riesgo aceptable.

Este nivel de riesgo aceptable tiene que estar aprobado por la Alta Dirección (Alcalde municipal y Secretario de Educación), y se tienen que definir los criterios para establecer dicho nivel.

Este cálculo del Riesgo total se obtendrá con la siguiente formula:

Riesgo = impacto potencial x frecuencia

Tabla 21. Modelo de capacidad CMM

EFECTIVIDAD	***CMM***	***SIGNIFICADO***	***DESCRIPIÓN***
0%	*L0*	*Inexistente*	*Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.*
10%	*L1*	*Inicial / Ad- hoc*	*Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.*
50%	*L2*	*Reproducible, pero intuitivo*	*Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada*

EFECTIVIDAD	*CMM*	*SIGNIFICADO*	*DESCRIPIÓN*
			individuo.
90%	*L3*	*Proceso definido*	*La organización entera participa en el proceso.* *Los procesos están implantados, documentados y comunicados mediante entrenamiento.*
95%	*L4*	*Gestionado y medible*	*Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos.* *Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.*
100%	*L5*	*Optimizado*	*Los procesos están bajo constante mejora.* *Con bases a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.*
50%	*L2*	*Reproducible, pero intuitivo*	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método.

EFECTIVIDAD	*CMM*	*SIGNIFICADO*	*DESCRIPIÓN*
			No hay comunicación o entrenamiento formal,las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	*L3*	*Proceso definido*	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados
EFECTIVIDAD	**CMM**	**SIGNIFICADO**	**DESCRIPIÓN**
95%	*L4*	*Gestionado y medible*	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	***L5***	***Optimizado***	*Los procesos están bajo constante mejora.* *Con base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los*

EFECTIVIDAD	*CMM*	*SIGNIFICADO*	*DESCRIPIÓN*
			procesos.

Fuente: Elaboración propia

Tabla 22. Nivel de riesgo aceptable y riesgo residual

ID	ACTIVO	FRECUENCIA		IMPACTO POTENCIAL					RIESGO				
				[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[L-01]	Oficina de Sistemas Municipio deYumbo	N	1	8	10	8	10	5	8	10	8	10	5
[HW-01]	Servidor Principal - Sistemas	F	10	8	10	10	10	10	80	100	100	100	100
[HW-02]	Servidor de Intranet - Sistemas	F	10	7	8	8	9	5	70	80	80	90	50
[HW-03 al 36]	Desktop No. 1 al Desktop No. 34	F	10	3	2	1	1	1	30	20	10	10	10
[HW-37]	Portátil	F	10	3	2	1	1	1	30	20	10	10	10
[SW-01]	Windows 7 Profesional	MF	100	5	2	5	5	3	500	200	500	500	300
[SW-02]	Windows 8 Profesional	MF	100	5	2	5	5	3	500	200	500	500	300
[SW-03]	Windows 8.1 Profesional	MF	100	5	2	5	5	3	500	200	500	500	300
[SW-04]	Windows 10 Profesional	MF	100	5	2	5	5	3	500	200	500	500	300
[SW-05]	Microsoft Office 2007 Profesional	MF	100	5	2	5	5	3	500	200	500	500	300
[SW-06]	Microsoft Office 2010 Profesional	MF	100	5	2	5	5	3	500	200	500	500	300
[SW-07]	Microsoft Office 2013 Profesional	MF	100	5	2	5	5	3	500	200	500	500	300
[SW-08]	Microsoft Office 2016 Profesional	MF	100	5	2	5	5	3	500	200	500	500	300
[SW-09]	Antivirus	MF	100	3	8	8	8	6	300	800	800	800	600

ID	ACTIVO	FRECUENCIA		IMPACTO POTENCIAL					RIESGO				
				[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[SW-10]	Windows Server 2008 R2	MF	100	7	9	9	8	8	700	900	900	800	800
[SW-11]	Linux	MF	100	3	8	9	3	7	300	800	900	300	700
[SW-12]	Aplicación **Help desk** Vs 0.90.3	MF	100	3	9	3	3	2	300	900	300	300	200
[SW-13]	Aplicación **Orfeo** 3.8.2	MF	100	2	8	9	8	7	200	800	900	800	700
[SW-14]	Aplicación **SRFPlus** Vs 3.0.62 R20070302	MF	100	2	8	9	8	7	200	800	900	800	700
[SW-15]	Aplicación Gestión de Matrícula **SIMAT**	MF	100	2	3	2	1	1	200	300	200	100	100
[SW-16]	Aplicación Gestión de Recursos Humanos **RRHH**	MF	100	3	2	1	1	1	300	200	100	100	100
[SW-17]	Aplicación Gestión y Control Financiero **SGCF**	MF	100	2	3	4	1	3	200	300	400	100	300
[D-01]	Datos de Empleados, Docentes, Estudiantes, Rectores, Personal Administrativo, Padres de familia, Establecimientos Educativos	MF	100	5	9	9	8	6	500	900	900	800	600
[D-02]	Datos de gestión Administrativa, Contable y Financiera.	MF	100	7	8	8	9	5	700	800	800	900	500
[D-03]	Datos de soporte técnico	MF	100	3	2	1	2	1	300	200	100	200	100
[D-04]	Copias de Seguridad	MF	100	5	9	9	8	6	500	900	900	800	600
[D-05]	Logs	MF	100	5	9	9	8	6	500	900	900	800	600
[COM-01]	UTM Fortinet	MF	100	5	9	9	8	6	500	900	900	800	600

ID	ACTIVO	FRECUENCIA		IMPACTO POTENCIAL					RIESGO				
				[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[COM-02]	Rourter	MF	100	4	7	9	7	5	400	700	900	700	500
[COM-03]	Access Point	MF	100	4	7	9	7	5	400	700	900	700	500
[COM-04]	Red Cableada	MF	100	4	7	9	7	5	400	700	900	700	500
[COM-05]	Red inalámbrica	MF	100	4	7	9	7	5	400	700	900	700	500
[S-01]	Correo Electrónico	MF	100	3	6	6	3	5	300	600	600	300	500
[S-02]	Servicio Web	MF	100	3	2	3	5	5	300	200	300	500	500
[AUX-01]	Impresoras	N	1	0	0	0	4	0	0	0	0	4	0
[AUX-02]	UPS	N	1	8	9	9	9	8	8	9	9	9	8
[AUX-03]	Aire Acondicionado	N	1	3	2	3	5	5	3	2	3	5	5
[AUX-04]	Planta eléctrica	N	1	3	6	6	3	5	3	6	6	3	5
[AUX-05]	Archivadores	N	1	3	3	5	5	4	3	3	5	5	4
[P-01]	Líder de TI Alcaldía	MF	100	5	9	9	8	6	500	900	900	800	600
[P-02]	Líder de TI SEMI	MF	100	5	9	9	8	6	500	900	900	800	600
[P-03]	Demás personal de TI	MF	100	4	5	3	5	3	400	500	300	500	300
[P-04]	Empleados SEMY	MF	100	4	5	3	5	3	400	500	300	500	300
[P-05]	Comunidad	MF	100	4	5	3	5	3	400	500	300	500	300

Fuente: Elaboración propia

En la tabla se puede observar con fondo sombreado los activos con mayor riesgo.

- **Riesgo aceptable y riesgo residual**

Se propone a La Alta Dirección del Municipio de Yumbo, que el nivel de riesgo aceptable sea 200, que corresponde al Nivel Medio, por lo tanto, todo lo que esté por debajo de este nivel, se considerará como una amenaza no importante para el Municipio, que no será incluida para la asignación de controles y serán tratados como riesgos residuales. Todo valor superior a éste indica que se debe establecer controles que mitiguen el riesgo asociado.

Posteriormente de acuerdo a la criticidad de los riesgos sobre los activos se asignarán los controles que presenten mayor urgencia.

- **Controles**

Considerando que hasta el momento en el Municipio de Yumbo no se ha llevado a cabo un proceso formal de implementación de controles para el ambiente de TI, se iniciará en este aparte la selección de Controles de acuerdo al resultado de los riesgos determinados y que aparecen en el cuadro anterior. Para ello se ha tenido en cuenta los grupos de activos que se definieron por cada una de sus dimensiones y el riesgo que generaron. Se utilizan controles proporcionados por la Norma ISO/IEC 27002, para lo cual se estima acorde al Modelo de Madurez de la Capacidad (CMM):

A continuación, se relacionan los controles recomendados:

- **Controles ISO27002**
  - **Políticas de seguridad.**
    - Directrices de la Dirección en seguridad de la información.
    - Conjunto de políticas para la seguridad de la información.
    - Revisión de las políticas para la seguridad de la información.
  - **Aspectos organizativos de la seguridad de la información.**

- Organización interna.
- Asignación de responsabilidades para la seguridad de la información.
- Segregación de tareas.
- Contacto con las autoridades.
- Contacto con grupos de interés especial.
- Seguridad de la información en la gestión de proyectos.
- Dispositivos para movilidad y teletrabajo.
- Política de uso de dispositivos para movilidad.
- Teletrabajo

❖ **Seguridad ligada a los recursos humanos.**

- Antes de la contratación.
- Investigación de antecedentes.
- Términos y condiciones de contratación.
- Durante la contratación.
- Responsabilidades de gestión.
- Concienciación, educación y capacitación en seguridad de la información.
- Proceso disciplinario.
- Cese o cambio de puesto de trabajo.

❖ **Gestión de activos**

- Responsabilidad sobre los activos.
- Inventario de activos.
- Propiedad de los activos.
- Uso aceptable de los activos.

- Devolución de activos.
- Clasificación de la información.
- Directrices de clasificación.
- Etiquetado y manipulado de la información.
- Manipulación de activos.
- Manejo de los soportes de almacenamiento.
- Gestión de soportes extraíbles.

❖ **Control de accesos**

- Requisitos de negocio para el control de accesos.
- Política de control de accesos.
- Control de acceso a las redes y servicios asociados.
- Gestión de acceso de usuario.
- Gestión de altas/bajas en el registro de usuarios.
- Gestión de los derechos de acceso asignados a usuarios.
- Gestión de los derechos de acceso con privilegios especiales.
- Gestión de información confidencial de autenticación de usuarios.
- Revisión de los derechos de acceso de los usuarios.
- Retirada o adaptación de los derechos de acceso
- Responsabilidades del usuario.
- Uso de información confidencial para la autenticación.
- Control de acceso a sistemas y aplicaciones.
- Restricción del acceso a la información.
- Procedimientos seguros de inicio de sesión.

- Gestión de contraseñas de usuario.
- Uso de herramientas de administración de sistemas.
- Control de acceso al código fuente de los programas.

❖ **Cifrado.**

- Controles criptográficos.
- Política de uso de los controles criptográficos.
- Gestión de claves.

❖ **Seguridad física y ambiental**

- Áreas seguras.
- Perímetro de seguridad física.
- Controles físicos de entrada.
- Seguridad de oficinas, despachos y recursos.
- Protección contra las amenazas externas y ambientales.
- El trabajo en áreas seguras.
- Áreas de acceso público, carga y descarga.
- Seguridad de los equipos.
- Emplazamiento y protección de equipos.
- Instalaciones de suministro.
- Seguridad del cableado.
- Mantenimiento de los equipos.
- Salida de activos fuera de las dependencias de la empresa.
- Seguridad de los equipos y activos fuera de las instalaciones.
- Reutilización o retirada segura de dispositivos de almacenamiento.

- Equipo informático de usuario desatendido.
- Política de puesto de trabajo despejado y bloqueo de pantalla.

❖ **Seguridad en la operación**

- Responsabilidades y procedimientos de operación.
- Documentación de procedimientos de operación.
- Gestión de cambios.
- Gestión de capacidades.
- Separación de entornos de desarrollo, prueba y producción.
- Protección contra código malicioso.
- Controles contra el código malicioso.
- Copias de seguridad.
- Copias de seguridad de la información.
- Registro de actividad y supervisión.
- Registro y gestión de eventos de actividad.
- Protección de los registros de información.
- Registros de actividad del administrador y operador del sistema.
- Sincronización de relojes.
- Control del software en explotación.
- Instalación del software en sistemas en producción.
- Gestión de la vulnerabilidad técnica.
- Gestión de las vulnerabilidades técnicas.
- Restricciones en la instalación de software.
- Consideraciones de las auditorías de los sistemas de información.

- Controles de auditoría de los sistemas de información.

❖ **Seguridad en las telecomunicaciones**

- Gestión de la seguridad en las redes.
- Controles de red.
- Mecanismos de seguridad asociados a servicios en red.
- Segregación de redes.
- Intercambio de información con partes externas.
- Políticas y procedimientos de intercambio de información.
- Acuerdos de intercambio.
- Mensajería electrónica.
- Acuerdos de confidencialidad y secreto.

❖ **Adquisición, desarrollo y mantenimiento de los sistemas de información.**

- Requisitos de seguridad de los sistemas de información.
- Análisis y especificación de los requisitos de seguridad.
- Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- Protección de las transacciones por redes telemáticas.
- Seguridad en los procesos de desarrollo y soporte.
- Política de desarrollo seguro de software.
- Procedimientos de control de cambios en los sistemas.
- Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- Restricciones a los cambios en los paquetes de software.
- Uso de principios de ingeniería en protección de sistemas.
- Seguridad en entornos de desarrollo.

- Externalización del desarrollo de software.
- Pruebas de funcionalidad durante el desarrollo de los sistemas.
- Pruebas de aceptación.
- Datos de prueba.
- Protección de los datos utilizados en pruebas.

❖ **Relaciones con suministradores**

- Seguridad de la información en las relaciones con suministradores.
- Política de seguridad de la información para suministradores.
- Tratamiento del riesgo dentro de acuerdos de suministradores.
- Cadena de suministro en tecnologías de la información y comunicaciones.
- Gestión de la prestación del servicio por suministradores.
- Supervisión y revisión de los servicios prestados por terceros.
- Gestión de cambios en los servicios prestados por terceros.

❖ **Gestión de incidentes en la seguridad de la información**

- Gestión de incidentes de seguridad de la información y mejoras.
- Responsabilidades y procedimientos.
- Notificación de los eventos de seguridad de la información.
- Notificación de puntos débiles de la seguridad.
- Valoración de eventos de seguridad de la información y toma de decisiones.
- Respuesta a los incidentes de seguridad.
- Aprendizaje de los incidentes de seguridad de la información.
- Recopilación de evidencias.

❖ **Aspectos de seguridad de la información en la gestión de la continuidad del negocio.**

- Continuidad de la seguridad de la información.
- Planificación de la continuidad de la seguridad de la información.
- Implantación de la continuidad de la seguridad de la información.
- Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- Redundancias.
- Disponibilidad de instalaciones para el procesamiento de la información.

❖ **Cumplimiento**

- Cumplimiento de los requisitos legales y contractuales.
- Identificación de la legislación aplicable.
- Derechos de propiedad intelectual (DPI).
- Protección de los registros de la organización.
- Protección de datos y privacidad de la información personal.
- Regulación de los controles criptográficos.
- Revisiones de la seguridad de la información.
- Revisión independiente de la seguridad de la información.
- Cumplimiento de las políticas y normas de seguridad.
- Comprobación del cumplimiento

5.2.3.7 Analisis de resultados

Tomando como base la información recopilada producto del análisis de riesgos de los activos de información de la secretaría de Educación del Municipio de Yumbo, se concluye que se debe realizar una gestión prioritaria sobre el componente de software y aplicaciones, conservar y mejorar los controles de comunicaciones [COM], EQUIPOS [HW], Equipamiento Auxiliar

[AUX] y Personal [P], que el Municipio de Yumbo actualmente no había estimado controles adecuados para su protección.

5.2.3.8 Políticas de administración del riesgo

Una vez realizado el análisis de riesgos es conocido el nivel de exposición en que se encuentra la organización, para ello se plantea diferentes propuestas de mejora que ayuden a mitigar el riesgo actual, de igual forma se pretende dar cumplimiento en mayor parte a los requisitos de la norma.

El Plan de Seguridad planteado incidirá en la mejora relacionada con la gestión de la seguridad y también en posibles beneficios colaterales como puede ser la optimización de recursos, mejora en la gestión de procesos y tecnologías presentes en la organización analizada.

- **Plan de seguridad**

Es la razón de ser del presente proyecto y este documento hacer parte integral de él, como lo establece el modelo de seguridad y privacidad de la información del estado colombiano.

- **Identificación de proyectos de seguridad**

Teniendo en cuenta el análisis de seguridad realizado con anterioridad, actualmente se cuenta con los resultados de las actividades de análisis y tratamiento de riesgos y los conocimientos de técnicas y productos de seguridad que permiten deducir la necesidad de los siguientes proyectos de seguridad:

Tabla 23. Proyectos de Seguridad propuestos

Secuencia	**Descripción**
PS-001	Legalización e implementación de controles de Software de Infraestructura y de Gestión.
PS-002	Implementar Gestión de privilegios y Acceso a los aplicativos.
PS-003	Realizar el mejoramiento en el proceso de copias de seguridad.
PS-004	Realizar gestión de logs.
PS-005	Garantizar la continuidad del servicio en caso de no disponibilidad de quipos de comunicaciones.
PS-006	Garantizar la continuidad del servicio en caso de caída de las redes.
PS-007	Mejoramiento en el Servicio de Correos.
PS-008	Continuidad de los procesos ante la ausencia de personal.
PS-009	Continuidad del SGSI ante la ausencia de personal relacionado.
PS-010	Diseñar e implementar Políticas de seguridad de la información.
PS-011	Mejorar la organización de la seguridad de la información.
PS-012	Realizar la Gestión de los activos.
PS-013	Mejorar el Sistema de control de acceso físico al Datacenter
PS-014	Mejorar el Sistema de control físico de los equipos.

Secuencia	**Descripción**
PS-015	Implementar Políticas de relación con los proveedores.
PS-016	Implementar Políticas de incidentes de seguridad de la información.
PS-017	Implementar estrategia que permita dar cumplimiento de normativa legal y de la organización.
PS-018	Implementar estrategia que permita dar cumplimiento de auditorías al SGSI.
PS-019	Implementar un Plan de Continuidad de Negocio.

Fuente: Elaboración propia

El objetivo genérico de estos proyectos, consiste en ayudar a minimizar el riesgo actual en materia de seguridad de la información en la Secretaría de Educación de Yumbo y dar evolución al cumplimiento de la norma hasta un nivel adecuado y previamente acordado.

La relación de escenarios de impacto y/o riesgo que afronta: activos afectados, tipos de activos, amenazas afrontadas, valoración de activos y amenazas y niveles de impacto y riesgo, fueron tratados y definidos en el punto anterior del presente documento.

La dependencia responsable de su ejecución, será la Secretaria de Educación del Municipio de Yumbo, en su área de Tecnología de Información y comunicaciones, en coordinación con el Departamento Administrativo de Planeación e Informática de la Alcaldía de Yumbo.

El grupo de trabajo creado para el diseño del SGSI, diseñará un presupuesto acorde las exigencias de implementación de cada proyecto, para lo cual se realizará;

- Una estimación de costes, tanto económicos (De adquisición, de contratación, de implantación, de formación, entre otros) como de esfuerzo de realización, teniendo en cuenta:
- Una relación de subtareas a afrontar (Legales, técnicos, de desarrollo, de formación entre otras).
- Cambios en la normativa y desarrollo de procedimientos.
- Una estimación del tiempo de ejecución desde su arranque hasta su puesta en operación.
- Una estimación del estado de riesgo (impacto y riesgo residual).

5.2.4 Identificación de vulnerabilidades de los activos de información ante amenazas potenciales

La identificación de las vulnerabilidades se realiza mediante visitas a las instalaciones del área de informática del Municipio de Yumbo, en donde se efectuó inspección visual de los activos de información y la información suministrada por el Líder TIC.

5.2.4.1 Inspección visual de los activos de información (Datacenter 1)

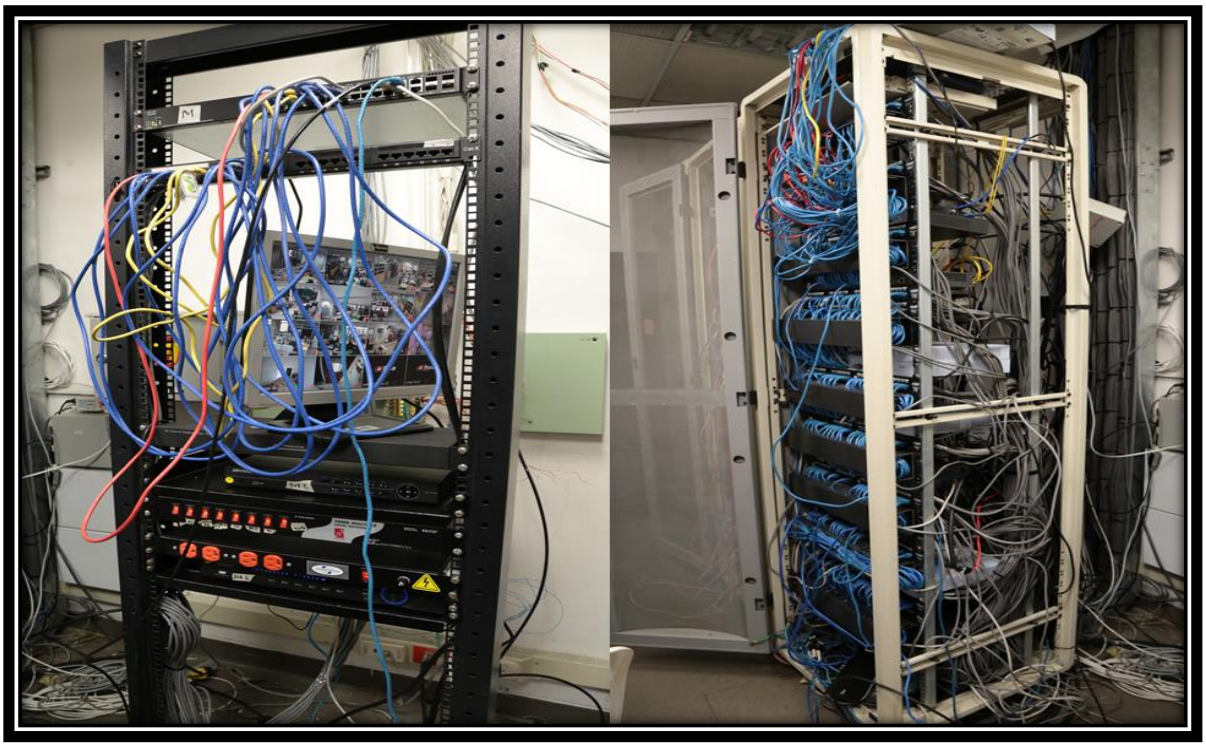
Figura 16. Puerta de acceso al Datacenter

Fuente: Imágenes propias del Area TIC de Yumbo.

- La entrada al Datacenter no cuenta con cámara de seguridad
- El control de acceso no dispone de un sistema biométrico o de seguridad, funciona con una cerradura de llave la cual no permite identificar al personal autorizado para ingresar al sitio. Existe un sistema lector de tarjetas deshabilitado.
- El área de TI no cuenta con un protocolo de acceso al Datacenter, como tampoco registro ni justificación de entrada y salida de personal.
- Las llaves son facilitadas por el líder TIC a cualquier técnico autorizado por el para su ingreso.

- El extintor contra incendios se encuentra obstruido por cajas en el suelo.

Figura 17. Racks de comunicaciones



Fuente: Imágenes propias del Area TIC de Yumbo.

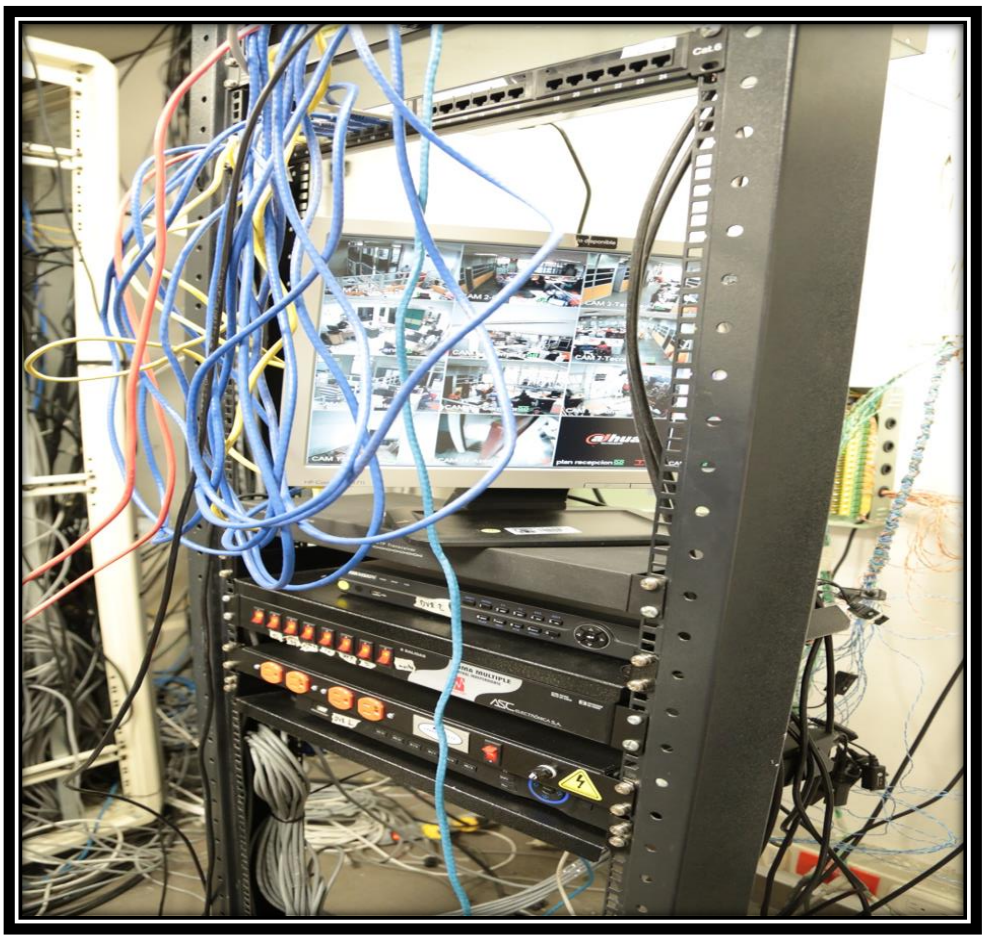
- Se encuentran que no hay una adecuada organización (paneles de obturación) ni identificación del cableado (marquillas), lo que dificulta la administración del mismo.
- Se evidencia que no se realiza aseo periódico ni adecuado, lo que puede implicar daños a los servidores y/o equipos de comunicación generados por la contaminación de polvo o suciedad.
- El área no cuenta con medidores de temperatura y humedad.
- Los rack están expuestos sin ninguna seguridad de acceso físico.

Figura 18. Racks de servidores

Fuente: Imágenes propias del Area TIC de Yumbo.

- Los rack están expuestos sin ninguna seguridad de acceso físico a los servidores.
- Los rack no cuentan con aisladores de emanaciones electromagnéticas.

Figura 19. Racks de Monitoreo de cámaras de seguridad



Fuente: Imágenes propias del Area TIC de Yumbo.

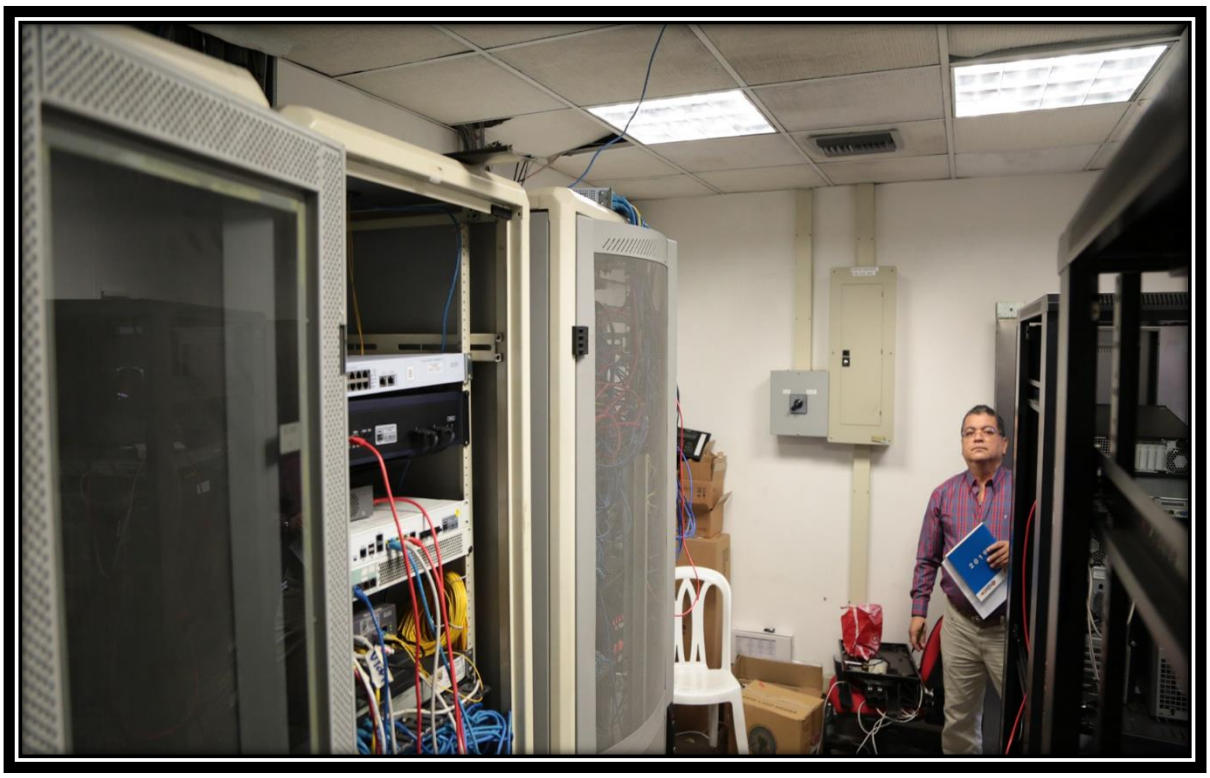
- El rack está expuesto sin ninguna seguridad de acceso físico.
- El monitor está oculto y expuesto.
- Se encuentran que no hay una adecuada organización (paneles de obturación) ni identificación del cableado (marquillas), lo que dificulta la administración del mismo.

Figura 20. Consola de Monitoreo de servidores

Fuente: Imágenes propias del Area TIC de Yumbo.

- El monitor está expuesto sin ninguna seguridad de acceso físico y colocado sobre un archivador.
- Se observa cableado expuesto y sin organización alguna.

Figura 21. Organización Datacenter 1

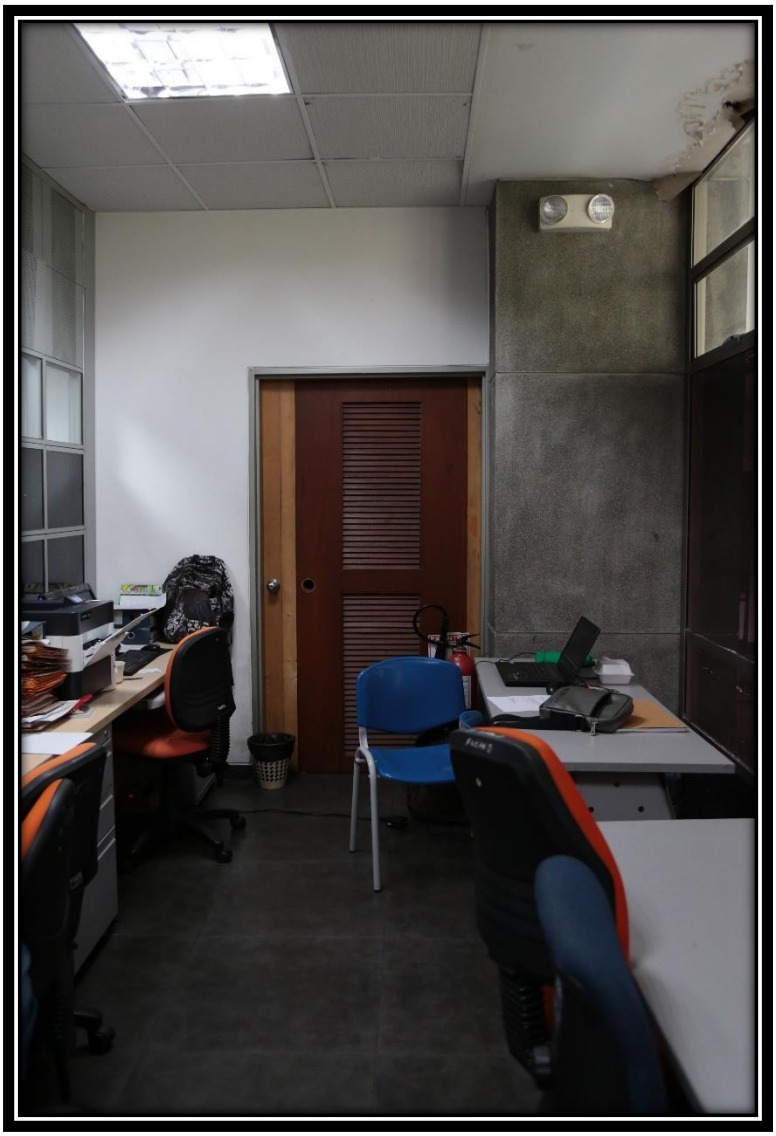


Fuente: Imágenes propias del Area TIC de Yumbo.

- En general se evidencia desorganización, cajas de cartón, cables expuestos, sillas, equipos sin uso en el suelo, algunos rack sin control de acceso, se cuenta con aire acondicionado central.

5.2.4.2 Datacenter 2

Figura 22. Puerta de acceso al Datacenter



Fuente: Imágenes propias del Area TIC de Yumbo.

- El ingreso al Datacenter se realiza pasando por un espacio asignado a la Secretaría de Educación de Yumbo al cual ingresan diferentes personas.
- El acceso al Datacenter se da mediante una puerta con una chapa sin llave y sin seguridad, quedando para el ingreso sin control de cualquier persona.
- La entrada al Datacenter no cuenta con cámara de seguridad.
- El control de acceso no dispone de un sistema biométrico o de seguridad.

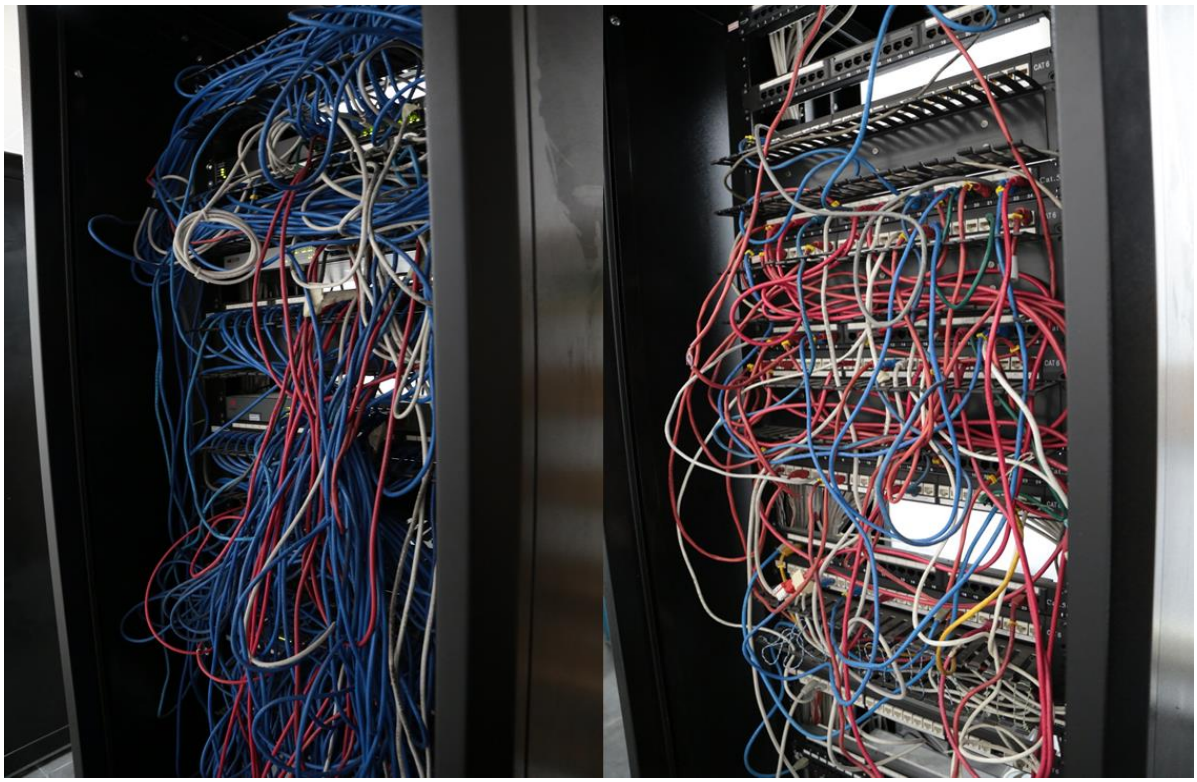
- El área de TI no cuenta con un protocolo de acceso al Datacenter 2, como tampoco registro ni justificación de entrada y salida de personal.

Figura 23. Organización del Datacenter 2

Fuente: Imágenes propias del Area TIC de Yumbo.

- El área se encuentra invadida por cajas con archivo de la Secretaría de educación, lo cual puede generar un riesgo de incendio.
- El aire acondicionado central no es el adecuado para un Datacente, genera probabilidad de riesgo de incendio por la temperatura de los equipos los cuales trabajan 7x24 los 365 días del año.
- No se cuenta con sensores de temperatura y humedad.
- Se encuentran dos UPS desconectadas.

Figura 24. Organización de los Rack de comunicaciones



Fuente: Imágenes propias del Area TIC de Yumbo.

- Se encuentran que no hay una adecuada organización (paneles de obturación) ni identificación del cableado (marquillas), lo que dificulta la administración del mismo.
- Se evidencia que no se realiza aseo periódico ni adecuado, lo que puede implicar daños a los equipos de comunicación generados por la contaminación de polvo o suciedad.
- El área no cuenta con medidores de temperatura y humedad.
- Los rack están expuestos sin ninguna seguridad de acceso físico.

5.2.4.3 Gestión de Activos

Figura 25. Aplicación de gestión de activos

Fuente: Imágenes propias.

- Se encuentran que existe un software para control de activos y están marcados los activos de información pero cada uno tienen diferentes placas, dificultando la administración y control sobre los mismos.

5.2.4.4 Control de acceso

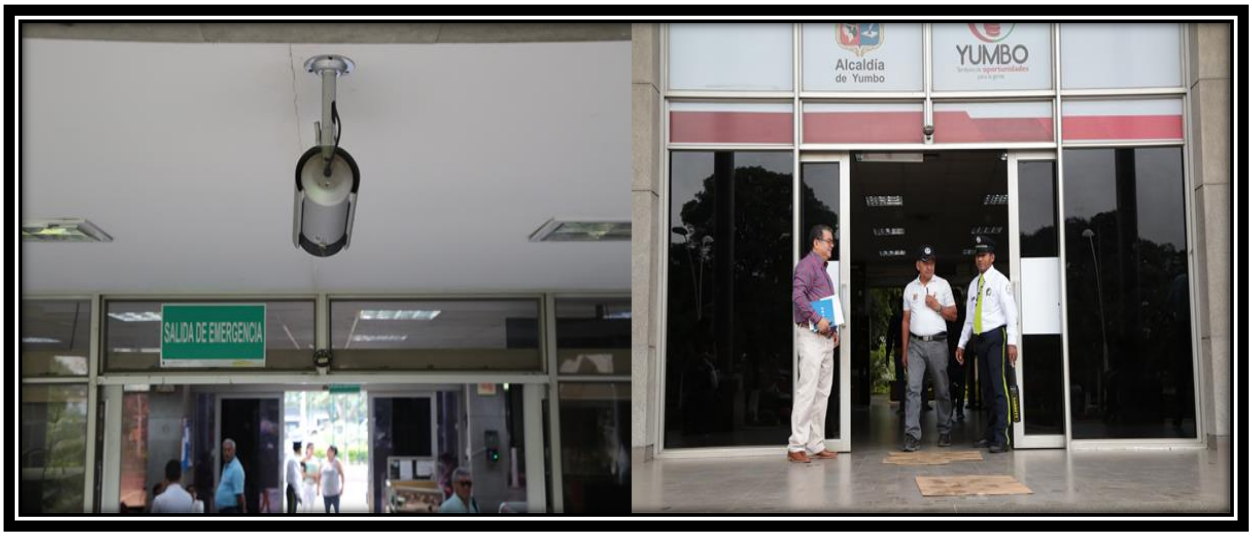
Figura 26. Control de acceso a la red de la Alcaldía de Yumbo

Fuente: Imágenes propias

- El control de acceso lógico a los recursos de la Alcaldía se realiza con base en la implementación de directorio activo de Microsoft Windows, pero desafortunadamente, varios usuarios comparten una misma clave, lo cual es un riesgo inminente para los sistemas de información.

5.2.4.5 Seguridad física y del entorno

Figura 27. Seguridad privada y cámaras de video vigilancia

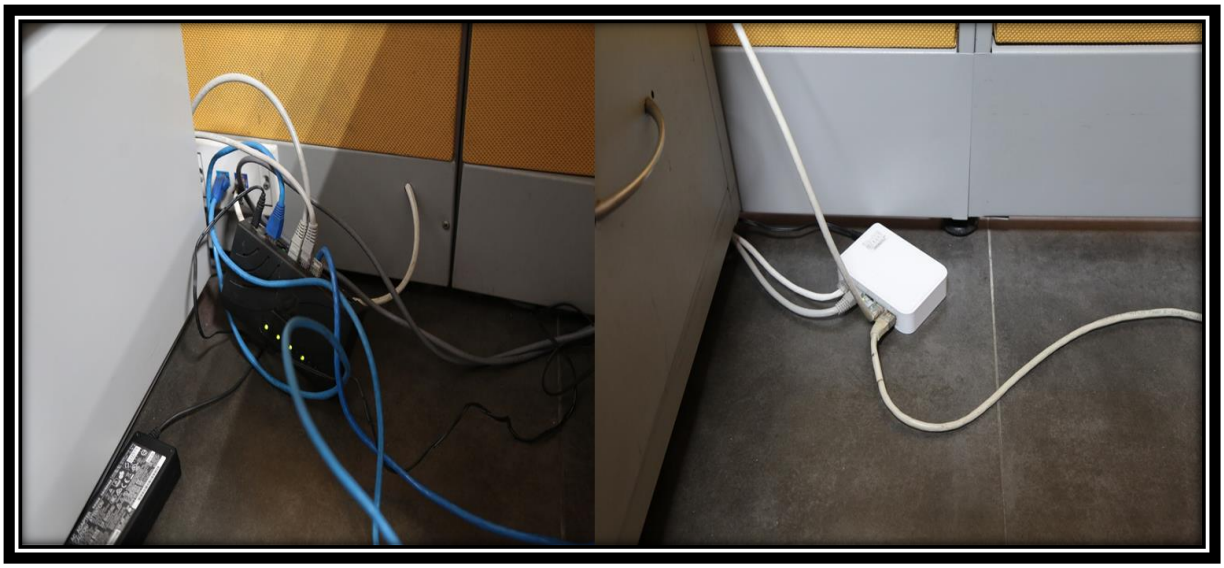


Fuente: Imágenes propias de la Alcaldía de Yumbo

- El control de acceso Físico a la Alcaldía tiene vigilancia privada pero no ejercen ningún control real a los visitantes.
- No se lleva registro de personas que ingresan y salen del Centro Administrativo Municipal.
- Existen algunas cámaras de seguridad ubicadas al interior de las oficinas y exterior pero no hay quien realice monitoreo y seguimiento permanente.

5.2.4.6 Seguridad de las Comunicaciones

Figura 28. Seguridad de las Comunicaciones



Fuente: Imágenes propias de la Alcaldía de Yumbo

- La inexistencia de políticas de seguridad y de control, hace que los usuarios de las diferentes dependencias de manera autónoma realicen instalaciones y derivaciones que ponen en riesgo los sistemas de información del Municipio de Yumbo.

5.2.4.7 Seguridad de las UPS

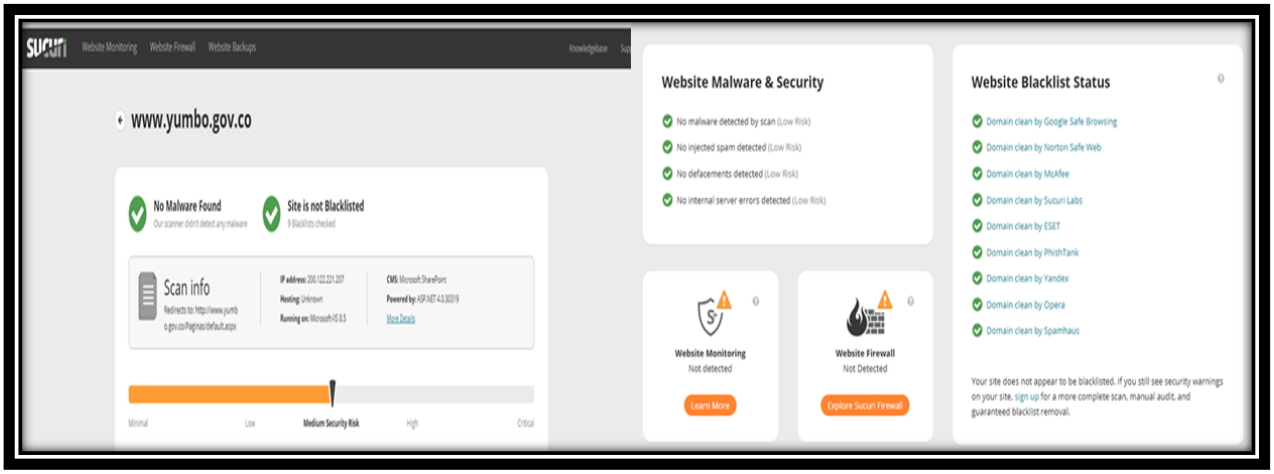
Figura 29. Seguridad UPS

Fuente: Imágenes propias de la Alcaldía de Yumbo

- El salón donde se encuentran ubicadas las UPS cuenta con aire acondicionado central, no tiene sensor de temperatura y humedad y una sola persona maneja las llaves lo cual es un alto riesgo ante cualquier contingencia.

5.2.4.8 Seguridad del sitio web www.yumbo.gov.co

Figura 30. Pruebas al portal www.yumbo.gov.co



Fuente: Imágenes propias de: https://sitecheck.sucuri.net/results/www.yumbo.gov.co

- Se realiza un scaneo del sitio web www.yumbo.gov.co, en busca de malware conocido, virus, estado de listas negras, errores del sitio web, software obsoleto y código malicioso, utilizando pare ello la herramienta online ubicada en https://sitecheck.sucuri.net/, encontrando que el sitio se encuentra en un nivel medio de riesgo de seguridad, no se ha configurado https, no se detectó malware por escaneo (bajo riesgo), no se detectó spam inyectado (bajo riesgo), no se han detectado desfiguraciones (bajo riesgo) y no se detectaron errores internos del servidor (bajo riesgo).
- El sitio web tiene asignada la dirección IP: 200.122.221.207 y se ejecuta en Microsoft-IIS 8.5, utiliza como CMS Microsoft SharePoint y fue desarrollado en ASP.NET 4.0.30319.

5.2.4.9 Evidencia prueba de otros controles

Teniendo en cuenta Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, como evidencia de lo manifestado en este proyecto frente a la situación actual de los

diferentes controles, se adjunta certificación del nuevo Líder TIC del Municipio de Yumbo, el cual hace parte del documento como Anexo 3.

Por lo anterior se propone la implementación de los siguientes insumos importantes para el Sistema de Gestión de la Seguridad del Municipio de Yumbo:

5.3. Política de seguridad y privacidad de la información

Este es un documento de alto nivel que manifiesta la voluntad de la Alta Dirección del Municipio de Yumbo, para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información MSPI.

La política propuesta contiene una declaración general por parte de la Administración Municipal en el cual se especifican los objetivos, alcance y nivel de cumplimiento en materia de Seguridad y Privacidad de la Información.

Para la realización de este documento se toma como referencia la guía del MinTIC denominada (Ministerio TIC de Colombia, 2016), en la cual se manifiesta " El siguiente documento es un formato que puede ser utilizado como plantilla para la elaboración de la política general de seguridad y privacidad de información para las entidades públicas, como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015".

A continuación, se detalla la política general propuesta:

5.3.1. Política general de seguridad y privacidad de la información del municipio de Yumbo

La Alta Dirección del Municipio de Yumbo, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión

de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el Municipio de Yumbo, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del Municipio de Yumbo

- Garantizar la continuidad del negocio frente a incidentes.
- El Municipio de Yumbo ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

5.3.2. Alcance/Aplicabilidad

Esta política aplica a todos los funcionarios, contratistas, terceros y partes interesadas de la entidad que en el ejercicio de sus funciones utilicen información y servicios TI del Municipio de Yumbo.

- **Objetivos**

De acuerdo con lo anterior, se establecen los siguientes objetivos de seguridad y privacidad de la información:

- Cumplir con los principios de privacidad y seguridad de la información.
- Dar cumplimiento a los principios de la función administrativa.
- Salvaguardar los activos de información.
- Definir políticas, procedimientos e instructivos en materia de seguridad y privacidad de la información.
- Establecer controles precisos para mantener la seguridad y privacidad de la información.
- Fijar las responsabilidades y autoridades de privacidad y seguridad de la información.
- Garantizar la gestión de riegos de la privacidad y seguridad de la información.
- Asegurar la gestión de incidentes de privacidad y seguridad de la información.

- Garantizar la continuidad del negocio y la recuperación ante desastres.
- Cumplir con las responsabilidades y obligaciones legales o contractuales.
- Establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información y el Modelo de Privacidad y Seguridad de la Información.
- Apoyar la innovación tecnológica.
- Mantener la confianza de los funcionarios, contratistas, terceros y partes interesadas.
- Fortalecer la cultura de privacidad y seguridad de la información en el Municipio de Yumbo.
- **Principios**

A continuación, se establecen los principios de seguridad que soportan el Sistema de Gestión de Seguridad de la Información y el Modelo de Privacidad y Seguridad de la Información del Municipio de Yumbo:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- El Municipio de Yumbo protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- El Municipio de Yumbo protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad

o en custodia.

- El Municipio de Yumbo protegerá su información de las amenazas originadas por parte del personal.
- El Municipio de Yumbo protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- El Municipio de Yumbo controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- El Municipio de Yumbo implementará control de acceso a la información, sistemas y recursos de red.
- El Municipio de Yumbo garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- El Municipio de Yumbo garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- El Municipio de Yumbo garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- El Municipio de Yumbo garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

- **Responsabilidades**

El personal encargado de la seguridad de la información es responsable de promover la privacidad y seguridad de la información en el Municipio de Yumbo.

La Alta Dirección del Municipio de Yumbo es responsable de garantizar que la seguridad y privacidad de la información se comunique y apropie adecuadamente en la entidad.

La Alta Dirección del Municipio de Yumbo es responsable de garantizar que la seguridad y privacidad de la información sean parte de la cultura organizacional.

Los funcionarios, contratistas, terceros y partes interesadas de la entidad tienen la responsabilidad

- **Resultado Clave**

Contar con un ambiente de seguridad y privacidad de la información en el Municipio de Yumbo, logrando el cumplimiento de los pilares de seguridad de la información que son la confidencialidad, integridad, disponibilidad y el no repudio; permitiendo como cabeza del Sector de Tecnologías de la Información y las Comunicaciones, apoyar y orientar a las demás entidades vinculadas y adscritas con los temas de privacidad y seguridad de la información y lograr su fortalecimiento.

- **Políticas relacionadas**

El manual de políticas generales de seguridad de la información del Ministerio TIC brinda los principios orientadores de seguridad de la información, estas directrices se encuentran alineadas a los controles del anexo A de la norma ISO 27001:2013, como son: organización de la seguridad de la información, seguridad del recurso humano, gestión de activos, control de acceso, criptografía, seguridad física y del entorno, seguridad de la operaciones, seguridad de la comunicaciones, adquisición, desarrollo y mantenimiento de sistemas, relaciones con proveedores, gestión

- **Cumplimiento**

Todos los funcionarios, contratistas, terceros y partes interesadas de la entidad que en el ejercicio de sus funciones utilicen información y servicios TI del Municipio de Yumbo deben cumplir con el 100% de la política. El incumplimiento de la política de seguridad y

privacidad de la información del Municipio de Yumbo, traerá consigo consecuencias legales de acuerdo a la normativa vigente.

5.4. Manual de política de seguridad y privacidad de la información

El presente manual describe los objetivos, alcances y el nivel de cumplimiento necesarios para garantizar el uso adecuado de los activos de información al interior de la Administración Municipal de Yumbo; definiendo responsabilidades y especificas en la gestión de la seguridad de la información. Para realizar e (MinTIC, 2016)

5.4.1. Objetivos y Alcance

5.4.1.1 Objetivo General

Establecer y difundir los criterios y comportamientos que deben seguir todos los funcionarios directos, temporales, contratistas, practicantes, terceros o cualquier persona que tenga una relación contractual con el Municipio de Yumbo, o que tenga acceso a los activos de información, con el propósito de preservar la Confidencialidad, Integridad y Disponibilidad de la información a fin de fortalecer la continuidad de las actividades administrativas, operativas y logísticas de la Entidad, protegiendo adecuadamente la información, reduciendo los riesgos y optimizando la inversión en tecnologías de información. Para tal efecto, se obrará en concordancia con las disposiciones legales vigentes. Como referencia para este documento se utiliza la guía No.3 Procedimientos de seguridad de la información de MinTIC, (2016), como también el Modelo de Seguridad y Privacidad de la Información de (MinTIC, 2016).

5.4.1.2 Objetivos Específicos

Se establecen los siguientes objetivos específicos:

- Proteger los recursos de información y tecnología frente a amenazas internas y externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la

confidencialidad, integridad y disponibilidad de la información, mediante la implementación de controles efectivos.

- Establecer un modelo organizacional de Seguridad de la Información, definiendo claramente los roles y responsabilidades de los que intervienen en la implementación de la política.
- Promover, mantener y realizar mejoramiento continuo del nivel de cultura en Seguridad de la Información, así como lograr la concientización de todos los funcionarios y contratistas y demás personas que interactúen con el Municipio de Yumbo, para minimizar la ocurrencia de incidentes de Seguridad de la Información.
- Mantener la política de Seguridad de la Información actualizada.

4.2.1.3 Alcance

El presente documento define la política, controles y directrices para el sistema de gestión de Seguridad de la Información del Municipio de Yumbo. La política establecida y sus posteriores actualizaciones aplican a todos los recursos y activos de información de la Entidad, así como a los designados para su uso y custodia.

5.4.2. Marco de referencia

5.4.2.1 Antecedentes

Teniendo en cuenta que la información es un activo vital para el éxito y el cumplimiento de la misión del Municipio de Yumbo, este documento se encuentra alineado con la familia de normas de la serie ISO 27000 como marco de referencia para la implementación de su sistema de gestión de Seguridad de la Información.

ISO 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco

de gestión de la Seguridad de la Información utilizable por cualquier tipo de organización. Entre las distintas normas que componen la serie ISO 27000 y que fueron tomadas como referente, se resalta ISO/IEC 27001 sobre los requisitos para el establecimiento del sistema de gestión de Seguridad de la Información.

La información, así como la plataforma tecnológica que la soporta, es considerada un activo estratégico para el Municipio de Yumbo, por lo que es fundamental establecer políticas que definan el marco de control para brindar seguridad a los activos de información de la Entidad. Estos activos de información se constituyen en el soporte de la misión y la visión, por lo que requieren ser utilizados y manejados dentro de un adecuado entorno de seguridad, cualquiera que sea el medio y el ambiente tecnológico en el que se encuentren.

Hoy por hoy, las organizaciones tanto públicas como privadas se están tornando altamente dependientes de sus sistemas de información y de los recursos informáticos que los soportan, por lo que se convierte en una decisión estratégica el implementar un Sistema de Gestión de Seguridad de la Información que esté directamente relacionado con las necesidades, objetivos institucionales y direccionamiento estratégico.

La implementación de un Sistema de Gestión de Seguridad de la Información está orientada a definir los aspectos necesarios para establecer, operar, mantener y dirigir de manera estandarizada, sistemática y organizada un sistema efectivo que permita el tratamiento seguro de la información.

5.4.2.2 Referencias normativas

- Ley 1266 de 2008 “Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información”.
- Ley 1273 de 2009 “Protección de la Información y de los Datos”.

- Documento CONPES 3701 de julio del 2011 “Lineamientos de política para ciberseguridad y ciberdefensa”.
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y su decreto reglamentario 1377 del 27 de junio de 2013.
- Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la República de Colombia.
- Resolución No. 03049 del 24 de agosto de 2012, por la cual se adopta el Manual del Sistema de Gestión de Seguridad de la Información.

Norma Técnica Colombiana NTC – ISO/IEC 27000

5.4.3. Misiones generales y particulares

5.4.3.1 Misión del Municipio de Yumbo

Mejorar la calidad de vida de la comunidad, cumpliendo los fines esenciales del Estado a través del manejo eficiente y ético de sus recursos; promoviendo los deberes, garantizando los derechos, la prestación de los servicios públicos, el desarrollo social, económico, ambiental y territorial, para la construcción del bien colectivo sostenible y sustentable.

5.4.3.2. Misiones particulares en materia de seguridad y privacidad de TI

5.4.3.2.1 Despacho del alcalde del Municipio de Yumbo

- Verificar el cumplimiento de la presente Directiva, en particular la difusión y adopción de las políticas, normas y estándares de Seguridad de la Información.
- Promover el desarrollo de una cultura de Seguridad de la Información a través de campañas de sensibilización y concientización.
- Implementar, apoyar y soportar el Sistema de Gestión de Seguridad de la Información.

- Apoyar los programas de capacitación, actualización y entrenamiento técnico del personal de las áreas de tecnología en temas relacionados con Seguridad de la Información.
- Gestionar los recursos financieros requeridos para la apropiada protección de los activos de información y mantenimiento del sistema de gestión de Seguridad de la Información.

5.4.3.2.2. Departamento administrativo de planeación informática área TIC

- Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de Seguridad de la Información.
- Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de Seguridad de la Información.
- Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de Seguridad de la Información.
- Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.
- Definir e implementar la estrategia de concientización y capacitación en Seguridad de la Información para los funcionarios, contratistas y demás terceros, cuando aplique.
- Custodiar la información y los medios de almacenamiento bajo su responsabilidad.
- Gestionar la plataforma tecnológica que soporta los procesos de la entidad.
- Definir, mantener y controlar la lista actualizada de software y aplicaciones autorizadas para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software base y de aplicaciones.
- Gestionar la adquisición de software y hardware.
- Asignar los equipos de cómputo a funcionarios y contratistas.

En cuanto a Seguridad de la Información se debe:

- Monitorear y evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.
- Establecer y dar mantenimiento a los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.
- Establecer, documentar y dar mantenimiento a los procedimientos de Seguridad de la información que apliquen para la plataforma de tecnologías de información administrada por esta oficina.
- Gestionar los incidentes de seguridad de la información que se presenten en la organización.

5.4.3.2.3 Secretaría de gestión humana y recursos físicos.

Incluir en los programas de inducción y de re-inducción el tema de seguridad de la información asegurando que los funcionarios conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de información o de otros recursos informáticos, haciendo énfasis en las consecuencias jurídicas que puede acarrear al servidor público.

5.4.3.2.4 Oficina de control interno.

Validar la aplicación y cumplimiento de las políticas de Seguridad de la Información definidas en esta Directiva, la aplicación de controles sobre los activos de información y los requerimientos del Sistema de Gestión de Seguridad de la Información.

- **Dueños de los procesos.** Definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados con sus procesos, incluyendo aquellas

actividades que sean consideradas como controles de Seguridad de la Información dentro de dichos procedimientos.

- **Propietarios de los activos de información**
- Los funcionarios y contratistas son responsables de la calidad de la información ingresada en los diferentes sistemas de información usados en la Municipio de Yumbo, para lo cual deben alimentar los datos que son editables en forma íntegra y veraz.
- Comunicar sus requerimientos de seguridad de información al líder del Área de Seguridad de la Información de la Oficina de Informática y Sistemas.
- Determinar y autorizar todos los privilegios de acceso a sus activos de información.
- Comunicar al Área de Seguridad de la Información sus requerimientos en capacitación sobre temas de seguridad.
- Participar en la resolución de los incidentes relacionados con el acceso no autorizado o con mala utilización de los activos de información bajo su responsabilidad, incluyendo los incumplimientos a la disponibilidad, confidencialidad e integridad.
- **Funcionarios, contratistas y terceros**
    - Cumplir con las políticas de Seguridad de la Información, contempladas en la presente directiva.
    - Velar por el cumplimiento de las políticas de Seguridad de la Información dentro de su entorno laboral inmediato.
    - Reportar de manera inmediata y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de Seguridad de la Información.
    - Utilizar los sistemas de información y el acceso a la red únicamente para los propósitos que lo vinculan.

- Utilizar únicamente software y demás recursos tecnológicos autorizados

5.4.4. Acciones que afectan la seguridad de la información

A continuación, se describen algunas acciones identificadas que afectan la Seguridad de la Información, y que ponen en riesgo su disponibilidad, confidencialidad e integridad:

- Dejar los computadores encendidos en horas no laborables.
- Permitir que personas ajenas a la Municipio de Yumbo ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible.
- No clasificar o etiquetar la información.
- No guardar bajo llave documentos impresos que contengan información clasificada al terminar la jornada laboral.
- No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
- Reutilizar papel que contenga información sensible, no borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo y no garantizar que no queden documentos o notas escritas sobre las mesas.
- Hacer uso de la red de datos del Municipio de Yumbo para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.
- Instalar software en la plataforma tecnológica del Municipio de Yumbo cuyo uso no esté autorizado por la Oficina de Informática y Sistemas, y que pueda atentar contra las leyes de derechos de autor o propiedad intelectual.

- Enviar información clasificada de la Entidad por correo físico, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Guardar información clasificada en cualquier dispositivo de almacenamiento que no pertenezca a la Municipio de Yumbo.
- Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos de la Entidad sin la debida autorización.
- Ingresar a la red de datos de la Entidad por cualquier servicio de acceso remoto sin la autorización de la Oficina de Informática y Sistemas.
- Usar servicios de internet en los equipos de la Entidad, diferente al provisto por la Oficina de Informática y Sistemas.
- Promoción o mantenimiento de actividades personales, o utilización de los recursos tecnológicos del Municipio de Yumbo para beneficio personal.
- Uso de la identidad institucional digital (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario o contratista.
- Dejar al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.
- Retirar de las instalaciones del Municipio de Yumbo computadores de escritorio, portátiles e información física o digital clasificada, sin autorización o abandonarla en lugares públicos o de fácil acceso.
- Entregar, enseñar o divulgar información clasificada del Municipio de Yumbo a personas o entidades no autorizadas.

- Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica de la Entidad o de terceras partes.
- Ejecutar cualquier acción que difame, afecte la reputación o imagen del Municipio de Yumbo, o alguno de sus funcionarios, utilizando para ello la plataforma tecnológica.
- Realizar cambios no autorizados en la Plataforma Tecnológica de la Entidad.
- Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.
- Ejecutar acciones para eludir y/o modificar los controles establecidos en la presente política de Seguridad de la Información.
- Consumir alimentos y bebidas, cerca de la plataforma tecnológica.
- Conectar a la corriente regulada dispositivos diferentes a equipos de cómputo.
- Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

La realización de alguna de estas prácticas u otras que afecten la Seguridad de la Información, acarrearán medidas administrativas, acciones disciplinarias o penales a que haya lugar, de acuerdo a los procedimientos establecidos para cada caso.

5.4.5. Procedimientos de seguridad y privacidad de la información

5.4.5.1 Seguridad del recurso humano

Este dominio está relacionado con la gestión de la seguridad de TI, aplicado al personal que labora en el Municipio de Yumbo y se proponen los siguientes procedimientos:

- **Procedimiento de capacitación y sensibilización del personal.**

El Municipio de Yumbo debe mantener un programa anual de concientización y capacitación para todos los funcionarios y contratistas que interactúen con la información institucional y

desarrollen actividades en sus instalaciones. Esto con el fin de proteger la información y la infraestructura tecnológica que la soporta.

Todos los funcionarios y contratistas al servicio del Municipio de Yumbo deben ser informados y capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas.

- **Procedimiento de ingreso y desvinculación del personal.**

El Municipio de Yumbo realiza la vinculación del personal de acuerdo a lo establecido por la normatividad vigente expedida por el Departamento Administrativo de la Función Pública (DAFP) y la ley 80 de contratación y Decretos reglamentarios.

Al momento de la desvinculación o cambio de roles en la Entidad, todo funcionario o contratista debe hacer entrega de todos los activos de información que le hayan sido asignados.

5.4.5.2 Gestión de activos

Este dominio está relacionado con la identificación y clasificación de activos de acuerdo a su criticidad y nivel de confidencialidad, se proponen los siguientes procedimientos:

- **Procedimiento de identificación y clasificación de activos.**

La información, los sistemas, las aplicaciones, los servicios y los equipos (equipos de escritorio, portátiles, impresoras, redes, Internet, dispositivos móviles, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) de todas y cada una de las dependencias y entidades del Municipio de Yumbo, son activos de información que se proporcionan a los funcionarios y contratistas para cumplir con sus respectivas actividades laborales. El Municipio de Yumbo se reserva el derecho de monitorear y supervisar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en la presente política.

a. El Municipio de Yumbo tiene la custodia sobre todo dato, información y mensaje generado, procesado y contenido por sus sistemas de cómputo, así como también de todo aquello transmitido a través de su red de telecomunicaciones o cualquier otro medio de comunicación físico o electrónico y se reserva el derecho de conceder el acceso a la información.
b. La Entidad debe identificar los activos asociados a cada sistema de información, sus respectivos propietarios y su ubicación a fin de elaborar y mantener un inventario actualizado de los activos de información.
c. La Entidad debe realizar la clasificación y control de activos con el objetivo de garantizar que los mismos reciban un apropiado nivel de protección, clasificar la información para señalar su sensibilidad y criticidad y definir los niveles de protección y medidas de tratamiento, evaluando las tres características de la información en las cuales se basa la Seguridad de la Información: confidencialidad, integridad y disponibilidad.
d. Debe realizar la clasificación de la información, evaluando las tres características de la información en las cuales se basa la seguridad de la información: confidencialidad, integridad y disponibilidad.
e. La Entidad deberá definir procedimientos para el rotulado y manejo de información de acuerdo al esquema de clasificación definido.
f. La Secretaría de Gestión Humana y Recursos físicos es la dependencia encargada de realizar la identificación, clasificación, asignación, marcado y digitalización de los activos de información, aplicando para ello la normatividad vigente en este sentido.

- **Uso de internet**

Internet es una herramienta de trabajo que permite navegar en sitios relacionados o no con las actividades diarias, por lo cual el uso adecuado de este recurso se controla, verifica y monitorea, considerando para todos los casos, las siguientes políticas:

a. La navegación en Internet estará controlada de acuerdo con las restricciones de navegación definidas para los usuarios; sin embargo, en ningún caso se considerarán aceptables los siguientes usos:

- Navegación en sitio de contenido sexualmente explícito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.
- Publicación, envío o adquisición de material sexualmente explícito, discriminatorio, que implique un delito informático o de cualquier otro contenido que se considere fuera de los límites permitidos.
- Publicación o envío de información confidencial sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.
- Utilización de otros servicios disponibles a través de Internet que permitan establecer conexiones o intercambios no autorizados por la Oficina de Informática y Sistemas.
- Publicación de anuncios comerciales o material publicitario, salvo la oficina de Comunicaciones cuando lo requiera. Estas solicitudes, deben ser justificadas por el jefe de la oficina de Comunicaciones y avaladas por el despacho del Superintendente.
- Promover o mantener asuntos o negocios personales.
- Descarga, instalación y utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el procesamiento de la estación de trabajo o de la red.

- Navegación en las cuentas de correo de carácter personal, no institucional, o en redes sociales, sin una justificación por parte de la entidad.
- Uso de herramientas de mensajería instantánea no autorizadas por la oficina de informática y sistemas.
- Emplear cuentas de correo externas no corporativas para el envío o recepción de información institucional.

b. Se realizará monitoreo permanente de tiempos de navegación y páginas visitadas por los funcionarios, contratistas y demás terceros autorizados. Así mismo, se puede inspeccionar, registrar e informar las actividades realizadas durante la navegación.

c. El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información

- **Uso del correo electrónico**

La asignación de una cuenta de correo electrónico del Municipio de Yumbo se da como herramienta de trabajo para cada uno de los funcionarios que la requieran para el desempeño de sus funciones, así como a contratistas y otros terceros previa autorización; su uso se encuentra sujeto a las siguientes reglas:

a. La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas en la Municipio de Yumbo.

b. Los mensajes y la información contenida en los buzones de correo son de propiedad de la Entidad y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

c. El tamaño de los buzones y mensajes de correo serán determinados por la Oficina de Informática y Sistemas.

d. No se considera aceptado el uso del correo electrónico de la Entidad para los siguientes fines:

- Enviar o retransmitir cadenas de correo, mensajes con contenido racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.
- Enviar mensajes no autorizados con contenido religioso o político.
- El envío de archivos adjuntos con extensiones como .mp3, .wav, .exe, .com, .dll, .bat, .msi o cualquier otro archivo que ponga en riesgo la Seguridad de la Información; en caso de que sea necesario hacer un envío de este tipo de archivos deberá ser autorizado por la Oficina de Informática y Sistemas.
- El envío masivo de mensajes corporativos deberá ser solicitado por el Jefe del Área que lo requiere y debe contar con la aprobación de la respectiva Oficina de Informática y Sistemas.

e. Toda información generada que requiera ser transmitida fuera de la Municipio de Yumbo, y que por sus características de confidencialidad e integridad debe ser protegida, debe estar en formatos no editables (PDF) y con mecanismos de seguridad (contraseñas). Sólo puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

f. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido y deben conservar, en todos los casos, el mensaje legal institucional de confidencialidad.

- **Uso de redes inalámbricas**

a. Los usuarios de las redes inalámbricas deben ser sometidos a las mismas condiciones de seguridad de las redes cableadas en lo que respecta identificación, autenticación, control de contenido de internet y cifrado entre otros.

b. La Oficina de Informática y Sistemas será la responsable de validar a quien se le asignarán los servicios a través de redes inalámbricas.

c. En ningún caso se podrá dejar configuraciones y contraseñas por defecto en los equipos inalámbricos.

- **Uso de computación en la nube**

a. Por ningún motivo se podrá almacenar información clasificada en servicios en la nube públicos o híbridos.

b. Ningún servicio de carácter misional, operativo o institucional del Municipio de Yumbo deberá ser contratado en Servicios en la Nube públicos o híbridos.

c. El Municipio de Yumbo podrá implementar servicios privados en la nube, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.

- **Sistemas de acceso público**

a. La información pública producida por las dependencias de la Entidad deberá estar resguardada de posibles modificaciones que afecten la imagen institucional.

b. El portal institucional deberá contener la política de privacidad y uso, así como la política de seguridad del mismo.

c. La Entidad deberá garantizar el derecho de Habeas Data al público que hace uso de los servicios de sus respectivos portales institucionales y propender por la Seguridad de la Información ingresada a través de ellos, aclarando que no se es responsable de la veracidad de la misma.

d. Toda la información publicada en el portal institucional o cualquier otro medio, deberá contar con la revisión y aprobación de la Oficina de Prensa y Comunicaciones.

- **Uso de recursos tecnológicos**

La asignación de los diferentes recursos tecnológicos se da como herramientas de trabajo para uso exclusivo de los funcionarios y contratistas. El uso adecuado de estos recursos se encuentra sujeto a las siguientes reglas:

a. La instalación de cualquier tipo de software en los equipos de cómputo es responsabilidad exclusiva de la Oficina de Informática y Sistemas, por tanto, son los únicos autorizados para realizar esta labor.

b. Ningún activo de información adquirido y que sea configurable, debe ser instalado con la configuración por defecto del fabricante o proveedor, incluyendo cuentas y claves de administrador.

c. Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla no definido. Estos cambios pueden ser realizados únicamente por la Oficina de Informática y Sistemas.

d. Los equipos de cómputo deberán ser bloqueados, por los usuarios que los tienen a cargo, cada vez que se retiren del puesto de trabajo.

e. Los requerimientos de recursos tecnológicos de las diferentes áreas deben ser avalados por la Oficina de Informática y Sistemas.

f. Los usuarios no deben realizar cambios físicos en las estaciones de trabajo, tales como, cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física. Estas actividades sólo podrán ser realizadas por la Oficina de Informática y Sistemas.

g. Los equipos de cómputo asignados deben ser devueltos a la dependencia responsable una vez sean reemplazados o cuando el funcionario o contratista responsable de dicho equipo finalice su vinculación con la Municipio de Yumbo.

h. De acuerdo con el literal anterior, la Entidad no debe almacenar equipos de cómputo en las oficinas una vez haya cesado el uso de los mismos.

4.2.5.3. Control de acceso

Este dominio está relacionado con el acceso a la información y a las instalaciones de procesamiento de la información, se proponen los siguientes procedimientos:

- **Procedimiento para Gestión de Terceros**

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica y que deban desarrollarse dentro de las instalaciones del Municipio de Yumbo, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar para el acceso a información sensible.

En ningún caso se otorgará acceso a terceros a la información sensible, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los

controles apropiados y se haya firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes o ambientes de computadores, contemplarán como mínimo los siguientes aspectos:

- Forma en los que se cumplirán los requisitos legales aplicables
- Medios para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, conocen sus responsabilidades en materia de seguridad
- Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos
- Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible
- Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres
- Niveles de seguridad física que se asignará al equipamiento tercerizado
- Derecho a la auditoría por parte de la Municipio de Yumbo
- **Acuerdos de confidencialidad**

Todos los funcionarios, contratistas y demás terceros deben firmar la cláusula o acuerdo de confidencialidad y este deberá ser parte integral de los contratos utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada, de acuerdo al formato de confidencialidad. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y a los recursos a personas o entidades externas.

- **Computación móvil**

a. Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se deben implementar controles de acceso y mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la Seguridad de la Información.

b. La conexión de los dispositivos móviles a la infraestructura tecnológica institucional deberá ser autorizada por la Oficina de Informática y Sistemas, previa verificación de que cuenten con las condiciones de seguridad y estableciendo mecanismos de control necesarios para proteger la infraestructura de la Entidad.

- **Control de acceso al data center**

a. El Data Center cuenta con un sistema de control de tarjeta de proximidad y clave para su ingreso. Además, cuenta con una cámara que graba únicamente cuando existe actividad al interior. Las personas que ingresan al Data Center quedan registradas en el software instalado en el equipo del administrador de red y el jefe de la Oficina de Informática y Sistemas.

b. Los sistemas de información, dispositivos de procesamiento y comunicaciones definidos por la Oficina de Informática y Sistemas contarán con mecanismos de identificación de usuarios y procedimientos para el control de acceso a los mismos.

c. Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad informática de la Entidad deberá estar autorizado por la respectiva Oficina de Informática y Sistemas.

d. Todas las conexiones remotas deberán ser autenticadas y seguras antes de conceder el acceso y el tráfico de datos deberá estar cifrado.

e. Todo identificador de usuario establecido para un tercero o contratista, debe tener una fecha de vencimiento especificada, la cual en ningún caso debe superar la fecha de sus obligaciones contractuales.

f. La asignación de privilegios en las aplicaciones para los diferentes identificadores de usuario estarán determinados por La Oficina de Informática y Sistemas y deben revisarse a intervalos regulares y modificar o reasignar estos cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.

g. Los equipos de contratistas y demás terceros que requieran acceder a las redes de datos de la Entidad deben cumplir un procedimiento de verificación antes de concedérseles dicho acceso.

h. Los equipos de contratistas y demás terceros que hayan sido autorizados para acceder de forma permanente a la red de la Entidad, sólo podrán hacerlo una vez se haya cumplido con el procedimiento inicial de formateo de discos duros y medios de almacenamiento, y posteriormente deben permanecer dentro de las respectivas instalaciones hasta la finalización del contrato o las labores para las cuales estaba definido.

i. Los accesos a la red inalámbrica deberán ser autorizados por la respectiva Oficina de Informática y Sistemas, previa verificación de que cuenten con las condiciones de seguridad, estableciendo mecanismos de control necesarios para proteger la infraestructura de la Entidad.

- **Administración de contraseñas**

a. La administración, así como la entrega de las contraseñas a los usuarios deberá realizarse por la Oficina de Informática y Sistemas.

b. Los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

- Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
- Las contraseñas no deberán ser reveladas.
- Las contraseñas no se deberán escribir en ningún medio, excepto para los casos de administradores, cuando son entregadas en custodia de acuerdo con el procedimiento establecido por la Oficina de Informática y Sistemas.
- Los funcionarios y contratistas deben digitar siempre su usuario y contraseña para acceder a las diferentes aplicaciones de la Entidad; las contraseñas no se deben guardar de forma automática en los inicios de sesión de las aplicaciones (Correo Electrónico, Orfeo, etc); igualmente al terminar la jornada deben cerrar las sesiones abiertas antes de apagar el equipo.
- Es deber de cualquier funcionario y contratista reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

- **Bloqueo de sesión, escritorio y pantalla limpia**

a. En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar los medios que contengan información crítica protegida bajo llave.

b. Los usuarios deberán bloquear su estación cada vez que se retiren de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del usuario.

c. Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por la Entidad, el cual se activará automáticamente después del tiempo de inactividad definido por la Oficina de Informática y Sistemas, y se podrá desbloquear únicamente con la contraseña del usuario.

d. Los usuarios deberán retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.

e. No se deberá reutilizar papel que contenga información sensible.

f. Los usuarios no deberán almacenar en el escritorio de sus estaciones de trabajo documentos, accesos directos a los mismos o a sistemas de información sensibles.

Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto, debe estar presente en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.

5.4.5.3 Seguridad física y del entorno

Este dominio está relacionado con la prevención del acceso a áreas no autorizadas, el daño a la infraestructura, las instalaciones o de la información, se proponen los siguientes procedimientos:

- **Procedimiento para la seguridad física y ambiental**

a. Las áreas protegidas y el Centro de Datos se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por la Oficina de Informática y Sistemas, a fin de permitir el acceso solo a personal autorizado.

b. Para la selección de las áreas protegidas y la ubicación del Centro de Datos se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil y otras formas de desastres naturales o provocados por el hombre. También se

tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad de las instalaciones.

c. Las plataformas tecnológicas serán ubicadas y protegidas de tal manera que reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

d. El cableado de datos que se incluya en cualquier proyecto en las instalaciones de la Entidad debe ser categoría 7A.

e. El cableado de energía eléctrica y comunicaciones que transportan datos o brindan apoyo a los servicios de información estarán protegidos contra intercepción o daños.

f. Se deberá garantizar la seguridad física del Centro de Datos, incluyendo entre otros los siguientes subsistemas:

- Sistema Eléctrico suplementario
- Sistema de Control de Acceso
- Sistema de protección contra incendios

- **Administración y control de usuarios al datacenter**

La seguridad física es importante para el cuidado y protección de la información, por esto se han definido las siguientes reglas:

Los funcionarios y contratistas deben contar con una tarjeta de proximidad para el ingreso al DataCenter ubicado en el Departamento Administrativo de Planeación e Informática. Las tarjetas de proximidad las controla el Líder TIC de la Entidad, teniendo en cuenta el número de funcionarios vinculados a la Municipio de Yumbo y la caducidad de las actividades de los contratistas.

En el tercer piso se encuentra el DataCenter de la Entidad, donde los funcionarios registran su ingreso por medio de la Tarjeta de Proximidad. En la recepción de la Alcaldía de Yumbo se encuentra un vigilante de la empresa de seguridad privada, encargados del control del acceso de las personas a la Entidad.

La puerta que utiliza sistema de control de acceso deberá permanecer cerrada, y es responsabilidad de todos los funcionarios y contratistas evitar que la puerta se deje abierta. Las personas que tengan acceso al Datacenter serán definidas única y exclusivamente por la Oficina de Informática y Sistemas.

Se debe exigir a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado para ellos por el Municipio de Yumbo mientras permanezcan dentro de sus instalaciones.

Es responsabilidad de todos los funcionarios y contratistas borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo y garantizar que no queden documentos o notas escritas sobre las mesas.

Es responsabilidad de todos los funcionarios y contratistas acatar las normas de seguridad y mecanismos de control de acceso de la Entidad.

- **Trabajo en áreas protegidas**

  a. En las áreas donde se encuentren activos informáticos, se debe cumplir como mínimo con los siguientes lineamientos:

  - No se deben consumir alimentos ni bebidas.
  - No se deben ingresar elementos inflamables.
  - No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.

- No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
- No se permite el ingreso de equipos electrónicos, así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.

b. Las áreas protegidas deben contar con las condiciones ambientales que garanticen la correcta operación de los equipos y el estado de los medios que contienen información, así como un sistema de detección y control de incendios.

- **Seguridad y mantenimiento de los equipos**

a. Los equipos que hacen parte de la infraestructura tecnológica del Municipio de Yumbo deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado a los mismos.

b. La Entidad adoptará los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo entre otros.

c. Los funcionarios y contratistas velarán por el uso adecuado de los equipos de escritorio, portátiles y móviles que les hayan sido asignados, por lo tanto, dichos equipos no deberán ser prestados a personas ajenas o no autorizadas.

d. Se debe asegurar que, sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se realicen mantenimientos periódicos con el fin de que dichas actividades no se vean afectadas por obsolescencia. Por

lo tanto, revisará constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de sus fabricantes.

e. Los equipos portátiles deberán estar asegurados con la guaya o el mecanismo que se defina para su protección, sea dentro o fuera de las instalaciones de la Entidad.

f. La Entidad garantizará la existencia de pólizas o seguros para la reposición de los activos informáticos que respaldan los planes de contingencia y la continuidad de los servicios.

- **Seguridad de los equipos fuera de las instalaciones**

a. Los usuarios que requieran usar los equipos fuera de las instalaciones del Municipio de Yumbo, deben velar por la protección de los mismos sin dejarlos desatendidos en lugares públicos o privados en los que se puedan ver comprometidos la imagen o información del sector.

b. En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información sensible, se deberá realizar inmediatamente el respectivo reporte de acuerdo con el procedimiento Gestión de Incidentes de Seguridad y se deberá poner la denuncia ante la autoridad competente, si aplica.

Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones del Municipio de Yumbo, deberán contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitarán los recursos que no se requieren o puedan poner en riesgo la información que contiene.

- **Gestión de medios removibles**

a. Los medios de almacenamiento removibles como cintas, discos duros removibles, CDs, DVDs, medios impresos y dispositivos USB, entre otros, que contengan información institucional, deben ser controlados y físicamente protegidos.

b. La Entidad definirá los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas por la Oficina de Informática y Sistemas, en la plataforma tecnológica si es requerido para el cumplimiento de sus funciones.

c. Cada medio removible de almacenamiento deberá estar identificado de acuerdo con el tipo de información que almacene.

d. Para los procesos de baja, reutilización o garantías de los dispositivos que contengan medios de almacenamiento, se debe cumplir según sea el caso con la destrucción física del mismo o borrado seguro.

e. El tránsito o préstamo de medios removibles deberá ser autorizado por el propietario del activo de información.

- **Política de roles**

Para los procesos del manejo de activos de la información de la entidad se deben cumplir con los roles que se generan para las personas involucradas en el tratamiento de la información y los sistemas de información, constituidos con el fin del tratamiento de la información y justos resultados.

Los roles son:

a. Propietario legal

El Municipio de Yumbo debe ser propietario legal de los activos de información. Ningún individuo puede reclamar los derechos de propiedad intelectual de un activo de información, a menos que se acuerde y apruebe por la Administración de acuerdo contractual.

Las Responsabilidades del propietario de activos son los siguientes:

- Actualización de la información de registro de inventario de activos.
- Identificar el nivel de clasificación de los activos de información.
- Definición e implementación de las salvaguardas apropiadas para asegurar la confidencialidad, integridad y disponibilidad de la información de activos.
- Evaluación y seguimiento de medidas de seguridad para garantizar su cumplimiento y reporte de situaciones de incumplimiento.

b. Líder de información (Chief Information Officer - CIO)

El CIO es quien asegura que los procesos de planificación estratégica se lleven a cabo, de manera que se cumplan los requisitos de información y sistemas de apoyo e infraestructura; Además sean alineados con los requisitos legislativos y los objetivos estratégicos. El CIO asegura la información, está bajo la responsabilidad del líder TIC de la Alcaldía Municipal de Yumbo.

Es el líder para las políticas de seguridad y prácticas de gobierno para garantizar la calidad y la integridad de los recursos de información del organismo y el apoyo a los sistemas de TI.

El CIO es responsable de:

- Interpretar las necesidades de utilidad y de información, y los deseos de la organización y su traducción a las iniciativas de TIC.
- Establece la estrategia de la tecnología de la información y las comunicaciones y la gestión de la información.
- Busca que las TIC y la gestión de información de la inversión está alineada a los objetivos estratégicos de la organización.

- Procura que los proyectos y las iniciativas están alineados y coordinados para ofrecer el mejor servicio.
- Garantiza que la planificación de las TIC está integrada en la planificación de negocios.
- Identificar las oportunidades para el intercambio de información y la colaboración en proyectos e iniciativa.

- **Gestor de Información**

a. Proporciona asesoramiento especializado en relación con las prácticas de gestión de la información.
b. Contribuye a la dirección estratégica de la gestión de la información dentro de la Organización.
c. Coordinar el desarrollo y la aplicación de gestión de la información.
d. Genera Prácticas en las políticas, normas, directrices y procedimientos.
e. Ayuda a las unidades de negocio para definir y comprender sus responsabilidades en relación con gestión de la información.
f. Ayuda a las unidades de negocio para identificar sus necesidades y requisitos de información.
g. Trabaja con el CIO para planificar e implementar los sistemas de administrar eficazmente los activos de información de la Municipio de Yumbo.

- **Oficial de seguridad de la información (CEO)**

El oficial de seguridad de la información es responsable de desarrollar e implementar la política de seguridad de la información diseñada para proteger la información y el apoyo a cualquier sistema de información de cualquier acceso no autorizado, uso, divulgación, corrupción o destrucción.

El oficial de seguridad de la información deberá:

- Desarrollar políticas, procedimientos y normas para garantizar la seguridad, confidencialidad y la privacidad de la información que sea consistente con la información de la organización política de seguridad.
- Supervisar e informar sobre cualquier incidente de información por intrusión y activar las estrategias para evitar nuevos incidentes.
- Trabajar con custodios de información para asegurar que los activos de información están bien resguardados.
- Mantenimiento y conservación del activo como se define por el propietario de los activos de reinicio y recuperación del sistema.
- La implementación de cualquier cambio de acuerdo con el procedimiento de gestión de cambios de copia de seguridad de la información.
- Actualización de la información de registro de inventario de activos.
- Identificar el nivel de clasificación de los activos de información.
- Definición e implementación de las salvaguardas apropiadas para asegurar la confidencialidad, integridad y disponibilidad de la información de activos.
- Evaluación y seguimiento de medidas de seguridad para garantizar su cumplimiento y reporte situaciones de incumplimiento.
- autorizar el acceso a aquellos que tienen una necesidad comercial de la información, asegurar el acceso.
- Se retira de los que ya no tienen una necesidad comercial de la información.

4.2.5.5. Seguridad de las operaciones

Este dominio busca asegurar las operaciones correctas dentro de las instalaciones de procesamiento de información, se proponen los siguientes procedimientos:

- **Control de cambios operativos**
  a. Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte de la Oficina de Informática y Sistemas de la Entidad, y debe cumplir con una planificación y ejecución de pruebas que identifiquen riesgos e impactos potenciales asociados que puedan afectar su operación.
  b. Todos los cambios que se realicen sobre los sistemas de información y la infraestructura tecnológica deberán estar precedidas de la definición de los requerimientos, especificaciones y controles definidos en el procedimiento de Control de Cambios. Dicha definición deberá ser realizada teniendo en cuenta como mínimo la confidencialidad, integridad y disponibilidad de la información.
- **Control de versiones**
  a. Antes de la puesta en producción de una aplicación nueva, o de la modificación de las plataformas existentes, se debe asignar un número de edición o versión a la misma. Así, el número de versión se irá incrementando en cada cambio que se genere sobre la misma aplicación.
  b. El método de enumeración de las versiones deberá distinguir entre versiones en producción, en etapa de desarrollo, en etapa de pruebas o versión archivada.
  c. Todas las versiones deben ser almacenadas en bibliotecas, repositorios o directorios y deben contar con controles de acceso lógicos donde sólo se permita el acceso al personal autorizado.
  d. Periódicamente, las versiones que se encuentran en los ambientes de producción deben ser verificadas contra los repositorios y la documentación de los controles de cambio con el fin de determinar si los dos son congruentes. Si llegase a presentarse incongruencia en

la revisión realizada, esto será identificado como un incidente de seguridad y se atenderá de acuerdo con el procedimiento de Gestión de Incidentes de seguridad.

- **Separación de ambientes**

a. El Municipio de Yumbo proveerá los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica y física entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios que pudieran afectar su operación.

b. Los usuarios deberán utilizar diferentes perfiles para el ambiente de desarrollo, de pruebas y de producción; así mismo, se deberá asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.

c. No deberán realizarse pruebas, instalaciones o desarrollos de hardware o software directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información.

d. El ambiente de prueba debe emular el ambiente de producción lo más estrechamente posible.

e. No se permite la copia de información sensible desde el ambiente de producción al ambiente de pruebas; en caso de que sea estrictamente necesario, la copia debe ser previamente ofuscada y se deben implementar controles que garanticen que la confidencialidad de la información sea protegida y se elimine de forma segura después de su uso.

f. Se restringe el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor.

- **Protección contra software malicioso**

a. Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y Seguridad de la Información deberán estar protegidos mediante herramientas y software de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos dados por código malicioso.

b. Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización de la Oficina de Informática y Sistemas, y deberán ser actualizados permanentemente.

c. No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto-replicarse, dañar o afectar el desempeño de cualquier equipo o red institucional.

d. Todos los medios de almacenamiento que se conecten a equipos de la infraestructura de la Entidad deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la Seguridad de la Información.

e. El código móvil sólo podrá ser utilizado si proviene de sitios de confianza y es autorizado por la Oficina de Informática y Sistemas.

f. La Entidad será responsable de que sus usuarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas

Web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.

g. Los sistemas, equipos e información institucionales deberán ser revisados periódicamente para verificar que no haya presencia de código malicioso.

5.4.5.4. Seguridad de las comunicaciones

Este dominio busca el aseguramiento y la protección de la información a través de los diferentes servicios de comunicaciones de la organización, se proponen los siguientes procedimientos:

- **Segregación de funciones**

  a. Todas las personas que tengan acceso a la infraestructura tecnológica o a los sistemas de información, deben contar con una definición clara de los roles y funciones sobre estos para reducir y evitar el uso no autorizado o modificación no intencional sobre los activos de información.

  b. La segregación de funciones sobre la infraestructura tecnológica y sobre los sistemas de información deberá ser revisada periódicamente por la Oficina de Informática y Sistemas con el fin de mantener actualizada dicha información y acorde con la realidad de cada una de las dependencias de la Entidad.

- **Gestión de registros (Logs)**

  a. Tanto los sistemas de información que manejan información crítica, como los dispositivos de procesamiento, de red y de seguridad informática deberán generar registros de eventos (logs) que serán verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información.

b. El tiempo de retención de los logs estará dado por las condiciones específicas de cada sistema de información, recurso informático o dispositivo de red y por las leyes, normativas o regulaciones vigentes.

c. Todo aquel evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica deberá ser reportado a la Oficina de Informática y Sistemas mediante el procedimiento de Gestión de Incidentes de seguridad.

5.4.5.5 Adquisición, desarrollo y mantenimiento de sistemas de información

- **Derechos de propiedad intelectual**

a. La Entidad cumplirá con la reglamentación de propiedad intelectual, para lo cual implementarán los controles necesarios que garanticen el cumplimiento de dicha reglamentación.

b. No se permitirá el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.

c. Se permitirá el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.

d. Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

e. El desarrollo de software a la medida adquirido a terceras partes o realizados por funcionarios de la Entidad, serán de uso exclusivo del Municipio de Yumbo y la propiedad intelectual será de quien lo desarrolle.

5.4.5.6 Gestión de incidentes y seguridad de la información

a. Los funcionarios y contratistas de la Entidad deberán informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.
b. Para gestionar los incidentes de Seguridad de la Información deberá existir como mínimo un funcionario con conocimientos en el manejo de incidentes en las Áreas de Seguridad de la Información.
c. Para los casos en que los incidentes reportados requieran judicialización se deberá coordinar con los organismos que cuentan con función de policía judicial.
d. Se debe establecer y mantener actualizado un directorio de los funcionarios involucrados dentro del procedimiento de Gestión de Incidentes de Seguridad de la Información para la Entidad.
e. Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.
f. Las Áreas de Seguridad de la Información deben propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de Seguridad de la Información.

g. Los resultados de las investigaciones que involucren a los funcionarios de la Entidad deberán ser informados a las áreas de competencia.

h. La Entidad deberá establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de Seguridad de la Información.

5.4.5.7 Aspectos de seguridad de la información de la gestión de la continuidad de negocio

- **Continuidad de negocio**

a. La Seguridad de la Información es una prioridad y se incluye como parte de la gestión general de la continuidad del negocio y del compromiso de la Alta Dirección.

b. La Entidad deberá contar con un Plan de Recuperación ante Desastres (DRP) que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.

c. Para el Sector Defensa su activo más importante es el recurso humano y por lo tanto será su prioridad y objetivo principal establecer las estrategias para mantenerlo.

d. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, estarán incorporados y definidos en el Plan de Recuperación ante Desastres.

e. Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio al responsable de la gestión del plan de recuperación de desastres.

- **Administración de backups, recuperación y restauración de la información**

a. Todas las copias de respaldo de la Entidad deben ser incrementales. El denominado backup incremental sólo copia los datos que han variado desde la última operación de

cualquier tipo. Se suele utilizar la hora y fecha de modificación en los archivos, comparándola con la hora y fecha de la última copia. La aplicación de respaldo, identifica y registra la fecha y hora de realización de las operaciones, para identificar los archivos modificados. La ventaja de un backup incremental es que copia una menor cantidad de datos que un respaldo completo. Por ello, esas operaciones se realizan más rápido y exigen menos espacio de almacenamiento.

b. Se debe asegurar que la información definida en conjunto por la Oficina de Informática y Sistemas y las dependencias responsables de la misma, y que se encuentra contenida en la plataforma tecnológica de la Entidad, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad, según lo definido en el Procedimiento Gestión de Copias de Respaldo y recuperación. Es por esto que las aplicaciones alojadas en los servidores del centro de cómputo del Municipio de Yumbo se les realizarán copias de respaldo automáticas todos los días.
c. Los medios de las copias de respaldo se almacenarán localmente y en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.
d. Se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia.

e. Para garantizar que la información de los funcionarios y contratistas sea respaldada, es responsabilidad de cada uno mantener copia de la información que maneja.

f. La Oficina de Informática y Sistemas del Municipio de Yumbo, establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia e identificación, y definirá conjuntamente con las dependencias los períodos de retención de la misma.

g. Se debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada en el Data Center.

- **Gestión de vulnerabilidades técnicas**

a. La Oficina de Informática y Sistemas de la Entidad se encargará de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto definirá las herramientas y servicios necesarios.

b. La Oficina de Informática y Sistemas será responsable de proponer y ejecutar un programa de evaluación y gestión de vulnerabilidades que debe ser utilizado para la plataforma tecnológica de la Entidad.

c. No se permite a los usuarios de los activos informáticos, sin la autorización expresa de la Oficina de Informática y Sistemas, realizar o participar por iniciativa propia o de terceros, en pruebas de acceso o ataques activos o pasivos a los activos informáticos del Municipio de Yumbo, o a la utilización de los mismos para efectuar pruebas de vulnerabilidad o ataques a otros equipos o sistemas externos.

d. Los administradores de las plataformas y sistemas de información serán responsables de mantener protegida la infraestructura a su cargo de los riesgos derivados de las vulnerabilidades técnicas identificadas.
e. El Área de Seguridad de la Información de la Entidad realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.
f. Periódicamente, la correspondiente Área de Seguridad de la Información realizará una verificación de alertas de seguridad emitidas por organizaciones y foros de Seguridad de la Información de orden nacional como también internacional, con el fin de verificar la información más reciente que se encuentre disponible respecto a vulnerabilidades y eventos de seguridad que se hayan presentado o que sean susceptibles de ocurrencia.

La Oficina de Informática y Sistemas de la Entidad realizará las revisiones de las alertas de seguridad informadas y dado el caso en que las alertas sean válidas en el entorno de operación de las plataformas tecnológicas asociadas, se deberá definir por parte de dichas oficinas un plan de acción para mitigar el impacto de las mismas en los ambientes de producción y desarrollo de la infraestructura tecnológica.

5.4.6 Sanciones previstas por incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente política de seguridad, conforme a lo dispuesto por las normas, se realizarán las acciones correspondientes ante el o los organismos disciplinarios pertinentes.

Las sanciones solo pueden imponerse mediante un acto administrativo que así lo disponga, cumpliendo las formalidades impuestas por los preceptos constitucionales, la ley de procedimientos administrativos y demás normativas específicas aplicables.

Además de las sanciones disciplinarias o administrativas, la persona que no da debido cumplimiento a sus obligaciones puede incurrir también en responsabilidad civil o patrimonial,

cuando ocasiona un daño que debe ser indemnizado y en responsabilidad penal cuando su conducta constituye un comportamiento considerado delito por el código penal y leyes especiales.

5.5. Roles y responsabilidades de seguridad y privacidad de la información

Se refiere a la elaboración de un acto administrativo a través del cual se crea o se modifica las funciones del comité de gestión institucional, en donde se incluyan los temas de seguridad de la información en la entidad, en este se deberá designar el responsable de la seguridad de la información dentro de la entidad. Para realizar esta actividad se toma como referencia la Guía No. 4 – Roles y responsabilidades de seguridad y privacidad de la información, disponible en (MinTIC, 2016).

A continuación, se detalla el documento con los Roles y Responsabilidades propuesto:

5.5.1. Definición de roles y responsabilidades

Con la definición de roles y responsabilidades se pretende establecer las tareas que se asignarán a cada uno de los miembros del equipo Modelo de Seguridad y Privacidad de la Información (MSPI) del Municipio de Yumbo, permitiendo ésto asegurar que cada actividad establecida en la etapa de planeación del mismo, tenga un responsable y de igual forma que cada uno de los miembros del equipo responsable de la ejecución, entienda claramente sus roles y responsabilidades.

5.5.1.1 Identificación de los responsables

Se requiere que todos los Secretarios de Despacho de la Alcaldía de Yumbo, estén vinculados al proceso de desarrollo del MSPI, para que se garantice el apoyo desde su planeación y marcar un punto de partida de éxito con la implementación del modelo de gestión de seguridad de la información planteado para el Municipio de Yumbo.

Los funcionarios referenciados deben identificar, establecer y organizar el grupo de trabajo responsable para implementar el MSPI, definiendo el perfil y rol.

5.5.1.2 Equipo de gestión

El equipo de gestión del proyecto, se encargará de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el MSPI al interior de la Administración Municipal de Yumbo, como también realizar las actividades necesarias para una adecuada administración y sostenibilidad del mismo.

5.5.1.3 Perfiles y responsabilidades

A continuación, se sugiere el conjunto de integrantes para el equipo encargado de la implementación del MSPI en el Municipio de Yumbo:

Responsable de seguridad de la información en el Municipio de Yumbo

Se sugiere que la responsabilidad de la Implementación del MSPI y por ende de la seguridad de la información del Municipio de Yumbo este a cargo del Director Administrativo de Planeación e Informática, quien tendrá las siguientes responsabilidades:

- Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo
- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.
- Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.
- Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.

- Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.
- Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo
- Encarrilar el proyecto hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad.
- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
- Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.
- Trabajar de manera integrada con el grupo o áreas asignadas.
- Asegurar la calidad de los entregables y del proyecto en su totalidad.
- Velar por el mantenimiento de la documentación del proyecto, su custodia y protección.
- Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.
- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.

Dentro de la definición de responsables en cada uno de los Dominios del Marco de Arquitectura Empresarial para Colombia disponible en (MinTIC, 2018), está contemplado el papel del responsable de seguridad y privacidad de la información, como se ilustra en la siguiente tabla:

Tabla 24. Responsabilidades - marco de arquitectura empresarial

DOMINIO	RESPONSABILIDADES
SERVICIOS TECNOLÓGICOS	* Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. * Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. * Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. * Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. * Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. * Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
ESTRATEGIA TI	* Definir la estrategia informática que permita lograr los objetivos y minimizar los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.
GOBIERNO TI	* Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado de monitorear y gestionar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de información.
SISTEMAS DE INFORMACIÓN	* Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. * Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. * Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.

DOMINIO	RESPONSABILIDADES
DOMINIO	**RESPONSABILIDADES**
	investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. * Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
INFORMACIÓN	* Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. * Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.
USO Y APROPIACIÓN	* Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. * Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. * Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.

Fuente: MinTIC, (2016, p.1).

- **Equipo del proyecto**

A continuación, se relacionan los miembros recomendados para conformar el Equipo de Seguridad y Privacidad de la Información para el Municipio de Yumbo:

- Un representante del área de TIC.
- Un representante del área de Control Interno.
- Un representante del sistema de Gestión de Calidad.
- Un representante del área Jurídica.

- Un representante del área de Secretaría de Hacienda.
- Un representante del área de Gestión Humana y Recursos Físicos.
- Funcionarios, proveedores, y ciudadanos invitados

El equipo del proyecto propuesto tendrá las siguientes funciones:

- Apoyar al líder de proyecto al interior de la entidad.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto.
- Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura.
- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.
- Las que considere el líder del proyecto o el comité de seguridad de la entidad.

Se recomienda que la Secretaría de Gestión Humana y Recursos Físicos de la Alcaldía de Yumbo, sea la oficina responsable del tratamiento de datos personales, quien tendrá las siguientes responsabilidades:

- Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.
- Tramitar las consultas, solicitudes y reclamos.
- Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran.
- Respetar las condiciones de seguridad y privacidad de información del titular.
- Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.
- **Comité de seguridad**

Teniendo en cuenta que el Municipio de Yumbo expidió el Decreto 333 del 3 de diciembre de 2014 “Por medio del cual se crea EL COMITE DE GOBIERNO EN LINEA Y ANTITRAMITES DEL MUNICIPIO DE YUMBO VALLE Y se dictan otras disposiciones…”, se recomienda adicionar al mismo o a través de una resolución la conformación del Comité se Seguridad, para lo cual como lo plantea la guía No. 4 Roles y Responsabilidades, presenta la siguiente plantilla:

RESOLUCIÓN (número) de (Año)

"Por la cual se conforma el Comité de Seguridad de la Información de nombre de la entidad y se definen sus funciones"

El Alcalde del Municipio de Yumbo, en cumplimiento de sus atribuciones legales y Constitucionales, en especial las conferidas, en el decreto 2693 de 2012, el Manual para la implementación de la Estrategia de Gobierno en línea de la república de Colombia, en armonía con la Ley de delito informático 1273 de 2009, Ley 1341 2009 Ley de Tecnologías de la Información y las Comunicaciones y la Ley estatutaria 1581 de 2012 de la Protección de datos y

CONSIDERANDO

...Que en mérito de lo expuesto,

RESUELVE:

Artículo 1°. Conformación del Comité de Seguridad de la Información. Créase el Comité de

Seguridad de la Información de Nombre de la entidad. El Comité estará integrado así:

- Un representante del área de TIC.
- Un representante del área de Control Interno.

- Un representante del sistema de Gestión de Calidad.
- Un representante del área Jurídica.
- Un representante del área de Secretaría de Hacienda.
- Un representante del área de Gestión Humana y Recursos Físicos.

Podrá asistir el representante de la oficina o su delegado.

Parágrafo 1º. El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

Artículo 2º. Objetivo del Comité de Seguridad de la Información. El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

Artículo 3°. Funciones del comité. El Comité de Seguridad de la Información del Municipio de Yumbo, tendrá dentro de sus funciones las siguientes:

1. Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
2. Revisar los diagnósticos del estado de la seguridad de la información en Nombre de la entidad.
3. Acompañar e impulsar el desarrollo de proyectos de seguridad.
4. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de Nombre de la entidad.

5. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.

6. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.

7. Participar en la formulación y evaluación de planes de acción para mitigar y eliminar riesgos.

8. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.

9. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.

10. Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.

11. Las demás funciones inherentes a la naturaleza del Comité.

12. Parágrafo. Una vez conformado el Comité de Seguridad de la Información, este podrá expedir su reglamento, en el cual fijará el alcance de cada una de las funciones operativas señaladas en el presente artículo.

Artículo 5°. Secretaria Técnica: La Secretaría Técnica del Comité se definirá al interior del

Comité y el secretario elegido será remplazado cada Doce (12) meses.

Artículo 6°. Funciones de la Secretaría Técnica. Las funciones de la Secretaría Técnica serán las siguientes:

1. Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.

2. Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias

3. Remitir oportunamente a los miembros la agenda de cada comité.

4. Llevar la custodia y archivo de las actas y demás documentos soportes.

5. Servir de interlocutor entre terceros y el Comité.

6. Realizar seguimiento a los compromisos y tareas pendientes del Comité.

7. Presentar los informes que requiera el Comité.

8. Las demás que le sean asignadas por el Comité.

Artículo 7°. Reuniones del Comité de Seguridad de la Información. El Comité de Seguridad de la Información – deberá reunirse (según periodicidad definida por la entidad), previa convocatoria del Secretario Técnico del Comité.

Artículo 8°. Sesiones extraordinarias. Los miembros que conforman el Comité podrán ser citados a participar de sesiones extraordinarias de trabajo cuando sea necesario, de acuerdo a temas de riesgos, incidentes o afectaciones de continuidad dentro del Sistema de Gestión de Seguridad de la Información.

Artículo 9°. Vigencia y Derogatoria: La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE Y CÚMPLASE Dado en Yumbo, a los (número) días del mes de (Mes) de (Año)

Nombre del Alcalde

Alcalde Municipal de Yumbo Valle

Capítulo VI. Plan de comunicación, sensibilización y capacitación sobre la importancia de la seguridad y privacidad de la información

6.1. Presentación

El presente Plan de Comunicación, sensibilización y capacitación propuesto, incluye la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles de la Administración Municipal de Yumbo. Para realizar esta actividad se toma como referencia la Guía No. 14 – Plan de comunicación, sensibilización y capacitación, disponible en (MinTIC, 2016).

La guía establece que "Un programa efectivo de sensibilización, capacitación y comunicación en seguridad de la información debe explicar de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas y la información, que generalmente están plasmadas en las políticas y procedimientos de seguridad de la información que la Entidad, requiere que sean cumplidos por parte de todos los usuarios del sistema" y que cualquier incumplimiento a las políticas, debe llevar a la imposición de una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad correspondiente a su rol y responsabilidades dentro de la Entidad".

6.2 Justificación

El modelo de seguridad y privacidad de la información MSPI del estado colombiano, establece que un punto importante dentro de la fase de planificación, es la realización del plan de comunicaciones, el cual debe incluir la estrategia para que la seguridad de la información se convierta en cultura organizacional, que permita generar competencias y hábitos en todos los niveles (directivo, funcionarios, terceros) de la entidad Municipio de Yumbo.

El plan de comunicación, sensibilización y capacitación, es un programa efectivo que busca que todos los funcionarios de la Alcaldía de Yumbo cumplan las políticas de seguridad de la información mediante actividades, capacitaciones, talleres y socializaciones.

El plan de comunicación, sensibilización y capacitación sobre las políticas de seguridad se deben realizar teniendo en cuenta lo siguiente:

- Existe la mentalidad que no hay nada importante por proteger en su computador.
- Se tiene el concepto errado que la tecnología por si misma puede resolver los problemas de seguridad.
- Continuamente se generan nuevos métodos mediante engaños que buscan obtener información confidencial.
- Se deben conocer tanto las amenazas externas como las internas.

Debido a las anteriores razones, el plan de comunicación, sensibilización y capacitación se diseñó teniendo en cuenta los requerimientos exigidos por Gobierno en Línea, logrando que los funcionarios conozcan los motivos y razones que generan los diferentes tipos de incidentes en seguridad de la información que existen alrededor de cada uno y acojan las debidas precauciones recomendadas a través de las diferentes actividades de concienciación y sensibilización.

6.3. Objetivos

6.3.1. Objetivo general

Proponer un plan de capacitación, sensibilización y comunicación de la seguridad de la información, para así asegurar que todos los funcionarios del Municipio de Yumbo, cumpla con sus roles y responsabilidades de seguridad y privacidad de la información, buscando:

- Definir las necesidades de capacitación.
- Definir los temas para la capacitación en seguridad de la información, de acuerdo a las partes interesadas.

- Proponer estrategias para sensibilización y entrenamiento.

6.3.2. Objetivos específicos

- Diseñar un plan de capacitaciones.
- Dar a conocer los objetivos de la campaña.
- Captar la atención de los funcionarios para que interactúen con las actividades de Seguridad de la Información.
- Relacionar e interactuar la campaña con todos los requerimientos de la Estrategia de Gobierno en Línea.
- Concientizar al personal de la Alcaldía con talleres y capacitaciones con temas de seguridad de la información.

6.4 Actividades

A continuación, se describen las actividades ejecutadas para proponer el plan de comunicaciones:

6.4.1. Diseño del programa de comunicación, sensibilización y capacitación.

En esta fase se identifican las actividades necesarias para cumplir con las metas de entrenamiento de la entidad Municipio de Yumbo.

Lo primero que se realizó fue definir el modelo de administración del programa de entrenamiento y sensibilización, el cual es centralizado, lo anterior teniendo en cuenta que las políticas, la estrategia y la implementación son fijadas por el Municipio de Yumbo a través de la secretaría de gestión humana y recursos físicos con el apoyo del departamento administrativo de planeación e informática y luego distribuidos de igual manera a todas las dependencias de la administración municipal, para que sean aplicadas de manera homogénea en cada una.

6.4.2. Identificación de necesidades

Para identificar las necesidades se utiliza como método entrevistas a 3 directivos de la secretaria de educación del municipio de yumbo, como también a 20 usuarios finales, encontrando:

- El 100% de los directivos de la secretaría de educación, manifiestan desconocer las leyes y directivas del programa de seguridad, también reconocen de la importancia de esta temática.
- El 80% de los usuarios finales comparten la clave de usuario.
- El 100% de los técnicos conocen la clave de administrador.
- El 100% de los usuarios desconocen sobre temas de seguridad de la información y en especial, el alcance del tema.
- Se desconocen las políticas de seguridad y privacidad de la información
- No existe un procedimiento de copias de seguridad de la información por parte de los usuarios finales.
- Existe desconocimiento de las normas de seguridad informática
- Hay desconocimiento de la asignación adecuada de claves.
- Hay desentendimiento de las políticas de seguridad y protección de datos personales

Además, en visitas a cada una de las oficinas de la Alcaldía se apreciaron hábitos no adecuados en los sitios de trabajo, como:

- Consumo de líquidos y alimentos junto a los equipos de cómputo.
- Más de una persona conoce las claves de los Correos electrónicos institucionales.
- En el momento de abandonar el sitio de trabajo temporalmente no cierran sesión en sus equipos de cómputo.

- Es muy fácil adquirir las contraseñas de un usuario en la red de la entidad, de sus correos electrónicos y es muy fácil vulnerar los sistemas de seguridad y cifrado.
- En los puestos de trabajo se pueden encontrar contraseñas escritas en las agendas, pegadas en la pantalla o debajo del teclado.

6.4.3. Diseño del plan de capacitación y sensibilización

Una vez identificadas las necesidades de capacitación, se procede con la elaboración de la propuesta de capacitación, el cual consta de los siguientes elementos:

6.4.3.1. Políticas del plan de comunicación, sensibilización y capacitación.

Este plan de comunicación, sensibilización y capacitación está diseñado con base en las políticas de seguridad y privacidad de la información, ítem IV seguridad de los recursos humanos del manual de políticas de seguridad de la información aprobadas mediante Decreto 120 de 2016 para dar cumplimiento a los lineamientos del Ministerio de las TIC y Gobierno en Línea.

6.4.3.2 Roles y responsabilidades

La secretaría de gestión humana y recursos físicos con el apoyo del departamento administrativo de planeación e informática de la Alcaldía de Yumbo, liderarán las actividades del plan de sensibilización, comunicación y capacitación, quienes gestionarán la logística y presupuesto necesarios para el desarrollo de las actividades.

Temas y acciones de información y sensibilización. Algunos de los aspectos que se deben tratar en este plan de comunicación, sensibilización y capacitación:

- Uso de contraseñas.
- Protección contra los virus.
- Respetar la política de seguridad.

- Instrucciones al uso del correo electrónico.
- Buen uso de internet.
- Backup de la información.
- Pasos a seguir en caso de incidentes.
- Ingeniería social.
- Seguridad para los dispositivos USB.
- Indicar medidas se seguridad para el envío de información sensible o confidencial.
- Software permitido y no permitido.
- Seguridad de los equipos.

Se recomienda que los ponentes sean funcionarios del departamento administrativo de planeación e informática de yumbo en su grupo TIC, realizando exposiciones magistrales y prácticas, utilizando para ello equipos de cómputo y recursos visuales.

❖ **Talleres de capacitación para todo el personal**

- **Capacitación inductiva**: Orientada a facilitar la integración de nuevos trabajadores. Organizar programas de capacitación para el conocimiento de políticas, buen uso y aprovechamiento de recursos tecnológicos.
- **Capacitación preventiva**: Orientada a prever los cambios que se producen en el personal, preparar al personal para enfrentar con éxito nuevas formas de ataque cibernético, nuevos virus, cambios en la metodología de trabajo informático, actualizaciones e implementación de nuevos procesos en las asistencias tecnológicos de la entidad.
- **Capacitación correctiva**: Orientada a solucionar problemas identificados mediante los estudios de diagnóstico del sistema de seguridad de la información de la entidad.

a. Tema

Acciones seguras para proteger la información

b. Ponentes

Grupo TIC Alcaldía de Yumbo.

c. Metodología a utilizar

Exposición teórico y práctico utilizando recursos visuales

❖ **Desarrollo de material visual**

- Post de la campaña expectativa
- Imagen y nombre de la campaña
- Folletos: Se elaborarán folletos con información relativa a los temas de seguridad y privacidad de la información y gestión de riesgos.
- Afiches: Se elaborarán afiches en papel con la finalidad de generar expectativa e interés en las acciones emprendidas por la oficina de las TIC.
- Asignación de clave: Para enseñar a los funcionarios la forma correcta de asignar una contraseña tanto para correos electrónicos como para sistemas de información.
- Fondos y protectores de Pantalla: Enfatizar los temas tratados dentro de las políticas de seguridad de la información en la Alcaldía de Yumbo.
- Enlace (Link) en la página web de la Alcaldía de Yumbo: El documento con el plan de comunicación, sensibilización y capacitación de socialización, capacitación y comunicación se encontrará dispuesto en el link de gobierno en línea de la página institucional de la Alcaldía municipal de Yumbo www.yumbo.gov.co la finalidad que todas las personas, funcionarios de la entidad así como la comunidad en general tengan conocimiento de las actividades que contempla el plan de comunicación, sensibilización y capacitación .

Uso del correo institucional: Todas las actividades del plan de comunicación, sensibilización y capacitación de socialización, capacitación y comunicación serán informadas mediante correo electrónico institucional, así como todo material relacionado con las actividades de sensibilización.

- **Financiamiento del plan de comunicación, sensibilización y capacitación.** El financiamiento del Plan de Comunicación, Sensibilización y Capacitación, estará a cargo de la secretaría de gestión humana y recursos físicos en asocio de la oficina de prensa y comunicaciones de la Alcaldía de Yumbo.

- **Resultados y logros esperados.** Se tiene como resultados y logros esperados, informar, sensibilizar y comprometer al 100% de los funcionarios de la Alcaldía de Yumbo, sobre la implementación y fortalecimiento del Sistema de gestión de seguridad y privacidad de la información.

- **Evaluación.** La secretaría de gestión humana y recursos físicos en asocio con el departamento administrativo de planeación e informática de la alcaldía de Yumbo, se encargarán de evaluar el desarrollo de las acciones de capacitación y socialización, en función a los informes de evaluación y desarrollo.

La campaña de sensibilización a los diferentes grupos objetivo definidos, tendrá una duración mínima de 12 meses, que iniciarán con el plan de comunicación, sensibilización y capacitación, apoyo por medio de los afiches y folletos para dar a conocer masivamente la campaña para todo el personal de la entidad.

- **Colaboración con otras áreas.** Para llevar a cabo el plan de comunicación, sensibilización y capacitación dentro de la Alcaldía de Yumbo, se debe contar con el compromiso de todas las dependencias y en especial el apoyo de secretaría de gestión humana y

recursos físicos para la autorización de permisos, espacios de tiempo, sitios de reunión y refrigerios durante las actividades propias del plan de comunicación, sensibilización y capacitación.

Conclusiones

Después de ejecutado el proyecto denominado “plan de gestión de seguridad de la información para la secretaría de educación del municipio de yumbo, en cumplimiento de la estrategia de gobierno en línea de Colombia”, una vez aplicado el modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de Información y Comunicaciones de Colombia (MinTIC) se concluye:

La efectividad de la implementación de los controles según la norma ISO 27001:2013 en su anexo A en la Alcaldía de Yumbo tiene una calificación de 30, lo que indica que los procesos y los controles siguen un patrón regular, los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas, no hay formación ni comunicación formal sobre los procedimientos y estándares y hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.

Se evidenció que no existe una política de seguridad y privacidad de la información, por lo anterior se asignó una calificación de Cero (0), correspondiente a una evaluación de efectividad de control **Inexistente**, lo que conlleva a la necesidad de elaborarla, aprobarla y firmarla, como también la revisión y actualización de la misma periódicamente.

Se evidenció que los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores; Por lo anterior se asignó una calificación de Treinta (30), correspondiente a una evaluación de efectividad de control REPETIBLE, lo que implica la necesidad entre otros aspectos de establecer los roles y responsabilidades frente a la ciberseguridad.

Respecto a la seguridad de los recursos humanos se encontró que se aplica el procedimiento de contratación siguiendo lo estipulado en la ley 80 y normatividad correspondiente, pero no se registra en los contratos la cláusula de responsabilidad frente a la seguridad de la información, por lo anterior se asigna una calificación de Treinta y Uno (31) correspondiente a una evaluación de efectividad de control REPETIBLE, lo que implica la necesidad de que se ajuste el proceso de contratación y se incorpore en los contratos responsabilidades en cuanto a la seguridad de la información.

En la gestión de activos se encuentra que el Municipio de Yumbo cuenta con un aplicativo llamado SRFPLUS para gestionar los activos, pero se debe mejorar el proceso de etiqueteado y control sobre los mismos, por lo anterior se asignó una calificación de Cincuenta y Ocho (58) correspondiente a una evaluación de efectividad de control **Efectivo.**

Sobre el control de acceso se evidenció que en el Municipio de Yumbo esta implementado directorio activo y servidor de bases de datos con usuarios creados y seleccionados con sus perfiles y roles, para acceso a los sistemas de información de la Alcaldía y Secretaría de Educación, pero falta documentar la política de control de acceso y revisar la manera de asignar claves de administrador. Por lo anterior se asignó una calificación de Sesenta y Seis (66) correspondiente a una evaluación de efectividad de control GESTIONADO, lo que implica la necesidad de crear política de control de acceso y revisar y ajustar asignación de claves a usuarios.

En el proceso de implementación de la criptografía se pudo evidenciar que no existe una política sobre el uso de controles criptográficos para la protección de la información de los datos tributarios (Pagos) en el aplicativo Impuestos Pluss. Por lo anterior se asignó una calificación de Cero (0) correspondiente a una evaluación de efectividad de control Inexistente.

En lo concerniente a la seguridad física y del entorno se pudo evidenciar que actualmente no existen directrices relacionadas con los perímetros de seguridad física, el acceso al DataCenter se da mediante tarjeta de acceso y solo a personal autorizado, hay Seguridad Física con vigilancia privada y cámaras IP, falta identificar el DataCenter, no se identifican los elementos de resiliencia, no existe procedimiento para revisar trabajo en área segura, el Área de carga, descarga y despacho a cargo de operarios y del almacén el cual se encuentra ubicado externo a las instalaciones de la Alcaldía de Yumbo. Por lo anterior se asignó una calificación de Treinta y Nueve (39) correspondiente a una evaluación de efectividad de control **Repetible.**

Respecto a la seguridad de las operaciones entre otros aspectos se evidenció que las aplicaciones de misión crítica de la Alcaldía y de la secretaria de Educación de Yumbo son tercerizadas y se aplica claramente la gestión de cambios, sin embargo, no existe documentación al respecto. Por lo anterior se asignó una calificación de Treinta y Siete (37) correspondiente a una evaluación de efectividad de control **Repetible.**

En la seguridad de las comunicaciones se encuentra como evidencia que se gestiona el acceso a las redes de forma *ad hoc*, es decir basados en el conocimiento y experiencia de los ingenieros de sistemas adscritos al Departamento Administrativo de Planeación e Informática, lo anterior indica que no existen directrices para la gestión de seguridad de redes, tampoco para la seguridad de los servicios de red, están parcialmente implementadas VLAN y GPO, no existen políticas y procedimientos de transferencia de información, no existen acuerdos sobre transferencia de información, no existen directrices para mensajería electrónica (se maneja a través de un tercero la mensajería corporativa EMCALI), no existen acuerdos de confidencialidad (se referencian tangencialmente en contrato laboral). Por lo anterior se asigna una calificación de Treinta y Siete (37) correspondiente a una evaluación de efectividad de control **Repetible**.

En la adquisición, desarrollo y mantenimiento de sistemas se evidenció que en la actualidad la alcaldía de Yumbo tiene contratado el soporte y actualización de los sistemas de información tributario, financiero, inventarios y nómina, sin embargo, entre otros aspectos no existen directrices para análisis y especificaciones de requisitos de seguridad de la información. Por lo anterior se asignó una calificación de Quince (15) correspondiente a una evaluación de efectividad de control **Inicial**.

En el control de relación con los proveedores se evidencia que no existe una política de seguridad de la información para las relaciones con los proveedores, en la contratación se aplica lo establecido en la ley de contratación estatal (ley 80), se solicitan pólizas de garantía y cumplimiento que son verificados por supervisores de contrato. Por lo anterior se asignó una calificación de Cuarenta (40) correspondiente a una evaluación de efectividad de control **Repetible.**

Respecto al control de incidentes de seguridad de la información se evidenció que existe una herramienta para mesa de ayuda, pero no están establecidos los procedimientos para la planificación y preparación de respuesta a incidentes. Por lo anterior se asignó una calificación de Diez y Siete (17) correspondiente a una evaluación de efectividad de control Inicial.

En el control sobre los aspectos de seguridad de la información de la gestión de la continuidad del negocio, se evidenció que la entidad no cuenta con un BCP (Bussines Continuity Plan) o DRP (Disaster Recovery Plan). Actualmente se cuenta con personal encargado de la seguridad, soporte y mantenimiento de equipos y sistemas de información, pero es personal por contrato de prestación de servicios, no existen planes aprobados, procedimientos de respuesta y recuperación documentados. Se cuenta con procesos pequeños para la realización de pruebas (Como algunas bases de datos de pruebas y algunos servicios de pruebas). Por lo anterior se asignó una

calificación de Treinta (30) correspondiente a una evaluación de efectividad de control **Repetible,**

Sobre el control de cumplimiento se evidenció que se aplica la ley 80 de contratación, para su cumplimiento interactúan la oficina de gestión humana, control interno y control interno disciplinario, pero no existe política publicada sobre el cumplimiento de propiedad intelectual que defina el uso del software y de productos informáticos. Por lo anterior se asignó una calificación de Veinte (20) correspondiente a una evaluación de efectividad de control **Inicial.**

Para identificar las necesidades de capacitación y sensibilización sobre la seguridad y privacidad de la información, se utiliza como método entrevistas a 3 directivos de la secretaria de educación del municipio de yumbo, como también a 20 usuarios finales, encontrando que:

- El 100% de los directivos de la secretaría de educación, manifiestan desconocer las leyes y directivas del programa de seguridad, también reconocen de la importancia de esta temática.
- El 80% de los usuarios finales comparten la clave de usuario.
- El 100% de los técnicos conocen la clave de administrador.
- El 100% de los usuarios desconocen sobre temas de seguridad de la información y en especial, el alcance del tema.
- Se desconocen las políticas de seguridad y privacidad de la información
- No existe un procedimiento de copias de seguridad de la información por parte de los usuarios finales.
- Existe desconocimiento de las normas de seguridad informática
- Hay desconocimiento de la asignación adecuada de claves.
- Hay desentendimiento de las políticas de seguridad y protección de datos personales

Lo anterior justifica la necesidad de realizar un proceso de capacitación de los funcionarios en materia de seguridad y privacidad de la información.

Se entiende entonces que el presente proyecto se convierte en un insumo muy importante para la completar las fases de implementación del modelo MSPI por parte de la oficina de sistemas del Municipio de Yumbo, para reducir las brechas en cuanto a la situación actual versus la que se debe cumplir a la fecha según las directrices dadas por el MinTIC.

Referencias Bibliográficas

CEC-IAN. (20 de 04 de 2015). *Sistema de Gestión y Seguridad de la Información - SNAP*. Obtenido de https://www.youtube.com/watch?v=hqxPG6roels

Congreso de Colombia. (05 de 01 de 2009). *Ley 1273 de 2009*. Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Congreso de la república de Colombia. (27 de 02 de 2018). *LEY ESTATUTARIA 1581 DE 2012*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

DAFP. (09 de 2011). *Guía para la administración del riesgo*. Obtenido de http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

Departamento Administrativo de la Función Pública (DAFP). (09 de 2011). *Guía para la administración del riesgo.* Obtenido de https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

Departamento Administrativo de la Función Pública. (12 de 2014). *Guía para la Administración del Riesgo*. Obtenido de http://www.funcionpublica.gov.co/eva/capacidades-locales-para-la-paz/biblioteca-virtual/gestion-desempeno-institucional-meci-y-modelo-integrado-de-planeacion/guia_admon_riesgo

ESET. (2017). *ESET Security Report Latinoamérica 2017*. Obtenido de https://welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

Gobierno de España. (10 de 2012). *Magerit Versión 3 - Catalogo de Elementos*. Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

Gobierno de España. (2012,P.8). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los sistemas de Información.* Obtenido de https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

HENG. (14 de 03 de 2014). *SUPERHENG - Seguridad de la Información.* Obtenido de https://www.youtube.com/watch?v=I4FCl4RZpqY

ISACA. (2018). Protegiendo la información. *ISACA Journal V3*, 3.

ISO. (06 de 2011). *ISO/IEC 27005:2011.* Obtenido de https://www.iso.org/standard/56742.html

ISO 27000. (2018). *Sistema de gestión de la seguridad de la información*. Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Lopez, M. (07 de 12 de 2014). *EBIOS.* Obtenido de http://metodologiasanalisisriesgos.blogspot.com.co/2014/12/ebios.html

Martinez, I. (9 de 12 de 2015). *Seguridad de La iNformación.* Obtenido de https://www.youtube.com/watch?v=FmZit-EGVAo

Ministerio de Comercio, Industria y Turismo de Colombia. (27 de 06 de 2013, P.1). *Decreto 1377 de 2013*. Obtenido de http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf

Ministerio de Tecnologías de Información y Comunicaciones. (12 de 12 de 2014). *Decreto numero 2573 de 2014*. Obtenido de http://www.mintic.gov.co/portal/604/articles-14673_documento.pdf

Ministerio TIC de Colombia. (11 de 05 de 2016). *Elaboración de la política general de seguridad y privacidad de la información.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MinTIC. (13 de 04 de 2008). *Decreto 1151 de 2008.* Obtenido de http://www.mintic.gov.co/portal/604/w3-article-3643.html

MinTIC. (20 de 12 de 2012). *Decreto 2396 de 2012.* Obtenido de http://www.mintic.gov.co/portal/604/w3-article-3586.html

MinTIC. (12 de 12 de 2014). *Decreto 2573 de 2014.* Obtenido de https://www.mintic.gov.co/portal/604/articles-14673_documento.pdf

MinTIC. (26 de 05 de 2015). *Decreto número 1078 de 2015.* Obtenido de http://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

MinTIC. (29 de 04 de 2015). *G.ES.05 Diseño e implementación de una estrategia de seguridad de la información*. Obtenido de http://www.mintic.gov.co/arquitecturati/630/w3-article-9483.html

MinTIC. (25 de 04 de 2016). Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

MinTIC. (14 de 03 de 2016). *Controles de Seguridad y Privacidad de la Información.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

MinTIC. (11 de 05 de 2016). *Elaboración de la política general de seguridad y privacidad de la información.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MinTIC. (01 de 04 de 2016). *Guía de gestión de riesgos*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MinTIC. (01 de 04 de 2016). *Guía de gestión de riesgos.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MinTIC. (14 de 03 de 2016). *Guía No. 8 - Controles de Seguridad y Privacidad de la Información.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

MinTIC. (25 de 04 de 2016). *Guía No.4 - Roles y Responsabilidades.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

MinTIC. (15 de 03 de 2016). *Guía para la Gestión y Clasificación de Activos de Información.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

MinTIC. (29 de 07 de 2016). *Modelo de Seguridad y Privacidad de la Información.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MinTIC. (17 de 03 de 2016). *Plan de Capacitación, Sensibillización y Comunicación de Seguridad de la Información.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

MinTIC. (24 de 05 de 2016). *Procedimiento de seguridad de la información*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

MinTIC. (25 de 04 de 2016). *Roles y Responsabilidades.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

MinTIC. (25 de 08 de 2017). *Decreto 1413 de 2017.* Obtenido de http://www.mintic.gov.co/portal/604/w3-article-59399.html

MinTIC. (09 de 06 de 2017). *Herramienta de Diagnóstico de Seguridad y Privacidad de la Información.* Obtenido de https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

MinTIC. (2018). *Arquitectura TI Colombia.* Obtenido de https://www.mintic.gov.co/arquitecturati/630/w3-channel.html

MinTIC. (2018). *Seguridad Y Privacidad de la Información*. Obtenido de http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-8015.html

Municipio de Yumbo. (01 de 06 de 2016). *Acuerdo Plan de Desarrollo Municipal 2016-2019.* Obtenido de http://www.yumbo.gov.co/Transparencia/PlaneacionGestionyControl/Acuerdo%20Plan%20de%20Desarrollo%20Municipal%202016%20-%202019.pdf

Municipio de Yumbo. (22 de 11 de 2017). *Acuerdo 019 de 2017*. Obtenido de http://www.yumbo.gov.co/Transparencia/Normatividad/Acuerdo%20No%20019%20de%202017%20Noviembre%2022.pdf

Municipio de Yumbo. (23 de 11 de 2017). *Acuerdo 019 de 2017.* Obtenido de http://www.yumbo.gov.co/Transparencia/Normatividad/Acuerdo%20No%20019%20de%202017%20Noviembre%2022.pdf

Municipio de Yumbo. (2018). *Organigrama.* Obtenido de http://www.yumbo.gov.co/NuestraAlcaldia/Paginas/Organigrama.aspx

ONU. (2016). *UN E-Goverment Survey 2016.* Obtenido de https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Govermnet-Survey-2016

ONU. (2018). *Un llamado a la acción para proteger a ciudadanos, sector privado y gobierno.* Obtenido de https://www.oas.org/es/sms/cicte/awswhitepaper.pdf

Organización de estados Americanos OEA y AWS. (2018, P.9). *Un llamado a la acción para proteger a sector privado y gobierno.* Obtenido de http://www.oas.org/es/sms/cicte/awswhitepaper.pdf

Perez, J. C. (2016). En J. C. Perez, *Protección de datos y seguridad de la información* (pág. 276). Bogotá: Ediciones de la U.

PMG. (2018). *Modelo de Magerit.* Obtenido de https://www.pmg-ssi.com/wp-content/uploads/2015/03/diagrama-16.png

Portal de la Transparencia España. (30 de 12 de 2016). *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Título VI con rango de ley ordinaria)* . Obtenido de http://transparencia.gob.es/servicios-buscador/contenido/leyorganica.htm?id=NORMAT_EA000862211170&lang=es&fcAct=2016-12-30T08:14:37.800Z

Presidencia de Colombia. (17 de 10 de 2012). *Ley estatutaria 1581 de 2012.* Obtenido de http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

Sampieri, R. H. (2014). Metodología de la Investigación. México DF: Mc Graw Hill.

Secretaría de Educación Yumbo. (2018). *Organigrama.* Obtenido de http://semyumbo.gov.co/nuestra-entidad/organigrama/

Secretaria General de la Presidencia Chile. (28 de 08 de 1999). *Ley 19628*. Obtenido de https://www.leychile.cl/Consulta/listaresultadosavanzada?stringBusqueda=117%23norm

al%23on%7C%7C48%23normal%23on%7C%7C46%23normal%23%5B%7BLey+1962
8%7D%5D%23%28%29%7C%7C-2%23normal%23on&tipoNormaBA=&o=experta

Senado de la República de Colombia. (31 de 12 de 2008). *Ley estatutaria 1266 de 2008.* Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Software Engineering Institute. (05 de 2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk.* Obtenido de https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

SYMANTEC. (2018). *informe sobre las amenzas para la seguridad en internet de 2018.* Obtenido de https://www.symantec.com/es/es/security-center/threat-report

Anexos

Anexo 1. Carta de aceptación anteproyecto MinTIC

Código TRD: 321

Bogotá D.C.;

Señor
HAMES VARGAS POLANCO
hamesvargas@hotmail.com
hamesv@yumbo.gov.co
Yumbo - Valle

ASUNTO: Respuesta a su radicado con número 881223 Anteproyecto " Diagnóstico sobre la seguridad y privacidad de a información en la Secretaría de Educación del Municipio de Yumbo frente al cumplimiento de la Estrategia de Gobierno en Línea"

Cordial saludo:

De manera atenta le informo que una vez revisado el anteproyecto del asunto presentado como parte de los requisitos de condonación de su crédito adquirido como beneficiario de la primera convocatoria para financiar estudios de posgrados en gestión TI y seguridad de la información (especializaciones y maestrías) adelantada en el marco del convenio interadministrativo No. 426 de 2015, suscrito entre el Fondo de Tecnologías de la Información y las Comunicaciones - Fontic y el Instituto de Crédito Educativo y Estudios Técnicos en el Exterior "Mariano Ospina Pérez"- ICETEX; a través del cual se encuentran adelantando la Maestría en gestión de Tecnologías de la Información en la UNAD; este Ministerio emite concepto de VIABILIDAD y le invita a continuar con las actividades relacionadas en el cronograma planteado.

Así mismo le deseamos éxitos en la implementación del proyecto, solicitamos informar a este Ministerio sobre los avances del mismo y cumplir con la totalidad de requisitos establecidos en el reglamento operativo y la convocatoria para lograr la condonación de su crédito.

Cordialmente,

ORIGINAL FIRMADO

ANTONIO CARRILLO ROSAS
Coordinador G.T Seguridad y Privacidad de TI

Proyectó. Lucy E. Palacios

Ministerio de Tecnologías de la Información y las Comunicaciones
Edificio Murillo Toro, Carrera 8a, entre calles 12 y 13
Código Postal: 111711 - Bogotá, Colombia
T: +57 (1) 3445460 Fax: 57 (1) 344 2948

vive digital
para la gente

Anexo 2. Carta de presentación y aceptación Municipio de Yumbo

Alcaldía
de Yumbo

Yumbo, 17 de diciembre de 2018

Doctor
RAFAEL LONDOÑO CARANTON
Subdirector de Estándares y Arquitectura TI
Ministerio de Tecnologías de Información y Comunicación – MINTIC
E.S.D

Cordial saludo.

Asunto: Certificación de Recibo a Satisfacción de Proyecto de Grado

Por medio del presente certificamos que una vez revisado el proyecto denominado "PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA SECRETARÍA DE EDUCACION DEL MUNICIPIO DE YUMBO, EN CUMPLIMIENTO DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA DE COLOMBIA", realizado por el Ingeniero Hames Vargas Polanco, identificado con cédula de Ciudadanía No. 16.450.771 de Yumbo, como requisito para optar el título de Magister en Gestión de TI de la Universidad Nacional Abierta y a Distancia (UNAD), y quien se desempeña como profesional especializado (Líder TIC) adscrito a la Secretaría de Educación de Yumbo, encontramos que:

1. El ingeniero Vargas presenta informe escrito del proyecto en donde se desarrolla y propone el Plan de Seguridad y Privacidad de la Información referido, con los siguientes componentes: (Política general de seguridad y privacidad de la información, manual de políticas, roles y responsabilidades de seguridad y privacidad, inventario de activos de información, identificación, valoración y tratamiento de riesgos y plan de comunicación, sensibilización y capacitación en materia de seguridad y privacidad de la información).
2. Los resultados de este proyecto resultan ser pertinentes e insumo muy importante para la Secretaría de Educación Municipal y la Alcaldía Municipal de Yumbo (Valle), pues contribuye a la construcción del Sistema de Gestión de la Seguridad de La información del Municipio de Yumbo (SGSI), que a su vez permite aportar al cumplimiento de lo establecido por el Decreto 1008 del 14 de junio de 2018 "Política de Gobierno Digital" en materia de Seguridad y Privacidad de la Información.

Nos permitimos felicitar al Ingeniero Hames Vargas Polanco, a la Universidad Nacional Abierta y a Distancia (UNAD) y al Ministerio TIC de Colombia, por apoyar este tipo de proyectos que ayudan a la modernización del Estado y a un mejor País.

Atentamente,

IVAN RECALDE CORREA
Secretario de Educación Municipal

LUIS FELIPE RAMOS
Líder TIC Municipio de Yumbo

Elaboró: Carmenza Pizarro Ortiz

Calle 5 No. 4-40 Barrio Belalcazar
PBX: 8516800 - www.yumbo.gov.co
E-mail: alcaldeyumbo@yumbo.gov.co
NIT: 890.399.025-6 Cod Postal:760601

Anexo 3. Certificación nuevo Líder TIC Yumbo

Alcaldía
de Yumbo

El suscrito líder TIC del Municipio de Yumbo

Certifica:

1. Que actualmente no se cuenta con una política de seguridad de la información.
2. No se han definido formalmente roles y responsabilidades frente a la ciberseguridad.
3. No se han definido formalmente roles y responsabilidades para la detección de incidentes.
4. No existe un acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información, revisado y aprobado por la alta Dirección.
5. No existe un Sistema de Gestión de la Seguridad de la Información.
6. Los acuerdos contractuales con empleados y contratistas, no establecen responsabilidades en cuanto a la Seguridad de la información.
7. El Municipio de Yumbo cuenta con un software de inventario llamado SRF PLUS, en donde se registran todos los activos de la administración, también manejan un inventario manual, y marcan todos estos con placas, la Secretaria de Gestión Humana y Recursos Físicos se encarga de administrar los inventarios.
8. El Municipio de Yumbo esta implementado directorio activo y servidor de bases de datos con usuarios creados y seleccionados con sus perfiles y roles, para acceso a los sistemas de información de la Alcaldía y Secretaría de Educación, pero falta documentar la política de control de acceso y revisar la manera de asignar claves de administrador.
9. No existe una política sobre el uso de controles criptográficos para la protección de la información de los datos tributarios (Pagos) en el aplicativo Impuestos Pluss.
10. Se pudo evidenciar que actualmente no existen directrices relacionadas con los perímetros de seguridad física, el acceso al DataCenter 1 se da mediante tarjeta de acceso y solo a personal autorizado, el acceso al DataCenter 2 es libre pues no existe control de acceso, hay Seguridad Física con vigilancia privada y cámaras IP, falta

Calle 5 No. 4-40 Barrio Belalcazar
PBX: 6516600 - www.yumbo.gov.co
E-mail: alcaldeyumbo@yumbo.gov.co
NIT: 890.399.025-6 Cod Postal:760501

identificar el DataCenter, no se identifican los elementos de resiliencia, no existe procedimiento para revisar trabajo en área segura, el Área de carga, descarga y despacho a cargo de operarios y del almacén el cual se encuentra ubicado externo a las instalaciones de la Alcaldía de Yumbo.

11. Las aplicaciones de misión crítica de la Alcaldía y de la secretaria de Educación de Yumbo son tercerizadas y se aplica claramente la gestión de cambios, sin embargo, no existe documentación al respecto.
12. Existe una solución de antivirus (Sophos), pero no está actualizada.
13. No existen directrices para la gestión de seguridad de redes, tampoco para la seguridad de los servicios de red, están parcialmente implementadas VLAN y GPO, no existen Políticas y procedimientos de transferencia de información, no existen acuerdos sobre transferencia de información, no existen directrices para mensajería electrónica (se maneja a través de un tercero la mensajería corporativa EMCALI), no existen acuerdos de confidencialidad (se referencian tangencialmente en contrato laboral). Datacenter 2 sin gestión adecuada.
14. En la actualidad la alcaldía de Yumbo tiene contratado el soporte y actualización de los sistemas de información tributario, financiero, inventarios y nómina.
15. No existen directrices para análisis y especificaciones de requisitos de seguridad de la información como tampoco directrices para la seguridad de servicios de las aplicaciones en redes públicas.
16. No existe una política de seguridad de la información para las relaciones con los proveedores, en la contratación se aplica lo establecido en la ley de contratación estatal (ley 80), se solicitan pólizas de garantía y cumplimiento que son verificados por supervisores de contrato.
17. Existe una herramienta para mesa de ayuda, pero no están establecidos los procedimientos para la planificación y preparación de respuesta a incidentes.

Alcaldía
de Yumbo

18. El Municipio de Yumbo no cuenta con un BCP (Bussines Continuity Plan) como tampoco con un DRP (Disaster Recovery Plan). Actualmente se cuenta con personal encargado de la seguridad, soporte y mantenimiento de equipos y sistemas de información, pero es personal por contrato de prestación de servicios, no existen planes aprobados, procedimientos de respuesta y recuperación documentados.
19. Se aplica la ley 80 de contratación, para su cumplimiento interactúan la oficina de gestión humana, control interno y control interno disciplinario; no existe política publicada sobre el cumplimiento de propiedad intelectual que defina el uso del software y de productos informáticos: existen y están definidas las tablas de retención documental.

Para constancia se firma en Yumbo (Valle del Cauca), a los 30 días del mes de Mayo de 2019.

Atentamente,

LUIS HERNAN DIAZ CLAROS
Líder TIC